

Jan Killmeyer

Information Security Architecture

An Integrated Approach to Security in the Organization
Second Edition



Information Security Architecture

Second Edition

OTHER INFORMATION SECURITY BOOKS FROM AUERBACH

Asset Protection and Security Management Handbook

POA Publishing
ISBN: 0-8493-1603-0

Building a Global Information Assurance Program

Raymond J. Curts and Douglas E. Campbell
ISBN: 0-8493-1368-6

Building an Information Security Awareness Program

Mark B. Desman
ISBN: 0-8493-0116-5

Critical Incident Management

Alan B. Sternecker
ISBN: 0-8493-0010-X

Cyber Crime Investigator's Field Guide

Bruce Middleton
ISBN: 0-8493-1192-6

Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes

Albert J. Marcella, Jr. and Robert S. Greenfield
ISBN: 0-8493-0955-7

The Ethical Hack: A Framework for Business Value Penetration Testing

James S. Tiller
ISBN: 0-8493-1609-X

The Hacker's Handbook: The Strategy Behind Breaking into and Defending Networks

Susan Young and Dave Aitel
ISBN: 0-8493-0888-7

Information Security Architecture: An Integrated Approach to Security in the Organization

Jan Killmeyer Tudor
ISBN: 0-8493-9988-2

Information Security Fundamentals

Thomas R. Peltier
ISBN: 0-8493-1957-9

Information Security Management Handbook, 5th Edition

Harold F. Tipton and Micki Krause
ISBN: 0-8493-1997-8

Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management

Thomas R. Peltier
ISBN: 0-8493-1137-3

Information Security Risk Analysis, 2nd Edition

Thomas R. Peltier
ISBN: 0-8493-3346-6

Information Technology Control and Audit

Fredrick Gallegos, Daniel Manson,
and Sandra Allen-Senf
ISBN: 0-8493-9994-7

Investigator's Guide to Steganography

Gregory Kipper
ISBN: 0-8493-2433-5

Managing a Network Vulnerability Assessment

Thomas Peltier, Justin Peltier, and John A. Blackley
ISBN: 0-8493-1270-1

Network Perimeter Security: Building Defense In-Depth

Cliff Riggs
ISBN: 0-8493-1628-6

The Practical Guide to HIPAA Privacy and Security Compliance

Kevin Beaver and Rebecca Herold
ISBN: 0-8493-1953-6

A Practical Guide to Security Engineering and Information Assurance

Debra S. Herrmann
ISBN: 0-8493-1163-2

The Privacy Papers: Managing Technology, Consumer, Employee and Legislative Actions

Rebecca Herold
ISBN: 0-8493-1248-5

Public Key Infrastructure: Building Trusted Applications and Web Services

John R. Vacca
ISBN: 0-8493-0822-4

Securing and Controlling Cisco Routers

Peter T. Davis
ISBN: 0-8493-1290-6

Strategic Information Security

John Wylder
ISBN: 0-8493-2041-0

Surviving Security: How to Integrate People, Process, and Technology, Second Edition

Amanda Andress
ISBN: 0-8493-2042-9

A Technical Guide to IPSec Virtual Private Networks

James S. Tiller
ISBN: 0-8493-0876-3

Using the Common Criteria for IT Security Evaluation

Debra S. Herrmann
ISBN: 0-8493-1404-6

AUERBACH PUBLICATIONS

www.auerbach-publications.com

To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401

E-mail: orders@crcpress.com

Information Security Architecture

An Integrated Approach to
Security in the Organization
Second Edition

Jan Killmeyer



Auerbach Publications

Taylor & Francis Group
Boca Raton New York

Published in 2006 by
Auerbach Publications
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2006 by Taylor & Francis Group, LLC
Auerbach is an imprint of Taylor & Francis Group

No claim to original U.S. Government works
Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-10: 0-8493-1549-2 (Hardcover)
International Standard Book Number-13: 978-0-8493-1549-7 (Hardcover)
Library of Congress Card Number 00-040399

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

No part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC) 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Library of Congress Cataloging-in-Publication Data

Tudor, Jan Killmeyer

Information security architecture: an integrated approach to security in the organization / Jan Killmeyer Tudor.

p. cm.

Includes bibliographical references and index.

ISBN 0-8493-1549-2 (alk. paper)

1. Computer security. 2. Computer architecture. I. Title.

QA76.9.A25 T83 2000

005.8--dc21

00-040399

informa

Taylor & Francis Group
is the Academic Division of Informa plc.

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>

and the Auerbach Publications Web site at
<http://www.auerbach-publications.com>

Dedication

This book is dedicated to the memory of my father, Fred J. Killmeyer, Jr., and the honor of my mother, Gladys Killmeyer Gillespie, whose love, inspiration, and devotion to their children provided me with the courage to take on and complete the challenge of writing this book.

Contents

1 Information Security Architecture	1
Why an Architecture?	2
Incident.....	3
Client/Server Environments	6
Overview of Security Controls	11
The Threat	11
The Risks	12
Incident.....	12
The Controls	14
The Strategic Information Technology (IT) Plan	17
Summary	22
Getting Started.....	22
2 Security Organization / Infrastructure.....	25
Learning Objectives	25
The Security Organization.....	26
The Executive Committee for Security	29
The Chief Information Officer	29
The Chief Financial Officer	31
The Security Officer.....	32
The Security Team.....	33
Security Coordinators or Liaisons.....	35
Departmental Management	36
Network and Application Administrators	37
Human Resources	37
Legal Counsel	37
Help Desk.....	39
Audit	39
Internal Audit.....	39
External Audit.....	41
Component Audits	42
Compliance Audits.....	42
System Users	42
Centralized versus Decentralized Security Administration.....	43

Information and Resource Ownership	45
The Strategic Information Technology (IT) Plan	49
Chapter Summary	54
Getting Started: Project Management	56
Deliverables	71
Password Parameters	72
Notes	75
3 Security Policies, Standards, and Procedures	77
Introduction.....	77
Learning Objectives.....	77
The Information Security Policy	81
Information Security Policy Acknowledgment Form	82
Network Usage Policy	82
E-Mail Policy	83
Internet Policy.....	87
Internet Risk.....	88
Process for Change.....	90
Security Standards	91
Standards Organizations.....	92
Security Procedures	96
Chapter Summary.....	97
Getting Started	98
Notes	99
4 Security Baselines and Risk Assessments	101
Information Security Assessment: A Phased Approach	102
High-Level Security Assessment (Section I).....	103
Assessing the Organization of the Security Function.....	103
Assessing the Security Plan.....	104
Assessing Security Policies, Standards, and Procedures	104
Assessing Risk-Related Programs	104
Security Operations (Section II)	105
Security Monitoring	105
Computer Virus Controls	106
Microcomputer Security	107
Compliance with Legal and Regulatory Requirements.....	108
Computer Operations (Section III)	108
Physical and Environmental Security.....	108
Backup and Recovery.....	109
Computer Systems Management	110
Problem Management.....	110
Application Controls Assessments.....	111
Access Controls.....	112
Separation (or Segregation) of Duties	113
Audit Trails	114

Authentication	114
Application Development and Implementation	116
Change Management	117
Database Security	117
Network Assessments	119
Emergency Response	120
Remote Access	121
Gateways Separating the Corporate WAN and Lines of Business	122
Current and Future Internet Connections	122
Electronic Mail and the Virtual Office	123
Placement of WAN Resources at Client Sites	124
Operating System Security Assessment	125
Windows NT	125
Telecommunications Assessments	132
Summary	136
5 Security Awareness and Training Program.....	139
Program Objectives.....	139
Employees Recognize Their Responsibility for Protecting the Enterprise's Information Assets	139
Employees Understand the Value of Information Security	140
Employees Recognize Potential Violations and Know Who to Contact	142
Incident.....	142
Forms of Attack	143
The Level of Security Awareness among Existing Employees Remains High.....	146
Program Considerations.....	147
Effectiveness Is Based on Long-Term Commitment of Resources and Funding.....	147
Benefits Are Difficult to Measure in the Short Term	148
Scoping the Target Audience.....	149
Incident.....	151
Effectively Reaching the Target Audience	154
Security Organizations	159
Summary	160
Getting Started — Program Development.....	161
6 Compliance	165
Level One Compliance: The Component Owner	166
Level Two Compliance: The Audit Function	167
Level Three Compliance: The Security Team	172
Line of Business (LOB) Security Plan	173
Enterprise Management Tools	173
Summary	176

7 Pitfalls to an Effective ISA Program	179
Lack of a Project Sponsor and Executive Management Support	180
Executive-Level Responsibilities	180
Executive Management's Lack of Understanding of Realistic Risk	181
Lack of Resources	182
The Impact of Mergers and Acquisitions on Disparate Systems	183
Independent Operations throughout Business Units	186
Discord Between Mainframe versus Distributed Computing Cultures	188
Fostering Trust in the Organization	190
Mom-and-Pop Shop Beginnings	191
Third-Party and Remote Network Management	192
The Rate of Change in Technology	196
Summary	197
Getting Started	199
8 Computer Incident / Emergency Response	201
Introduction	201
Learning Objectives	201
CERT®/CC	203
CSIRT Goals and Responsibilities	203
Reactive Services	205
Alerts and Warnings	205
Incident Handling	206
Vulnerability Handling	207
Artifact Handling	207
Incident Response Handling Methodology	208
Reporting	209
Incident Classification	213
Triage	213
Identification	215
Incident Analysis	216
Incident Response	218
Incident Response Coordination	219
Key Organizations	220
Containment	221
Eradication	223
Recovery	224
Notification	224
Development of the CSIRT	226
Issues in Developing a CSIRT	230
Funding	230

Management Buy-In	231
Staffing and Training	231
Policy Development.....	233
Legal Issues	234
Reevaluation of CSIRT Operations	236
Chapter Summary	236
Getting Started.....	236
Notes	237
9 Conclusion.....	239

APPENDIXES

A-1 Information Security Policy	243
A-2 Information Security Policy Acknowledgment Form	259
A-3 Network Computing Policy	263
A-4 E-Mail Security Policy	267
A-5 Internet Policy	271
A-6 Security Lists	275
A-7 Security Standards and Procedures Manual Table of Contents ...	277
A-8 Anti-Virus Update Procedure	283
B-1 Security Assessment Workplan	287
B-2 Application Security Assessment.....	301
B-3 Network Security Assessment Workplan.....	309
B-4 Windows NT Assessment Workplan	321
B-5 Telecommunications Security Assessment Workplan	327
C-1 Computer Incident/Emergency Response Plan	331
C-2 Sample Line of Business Security Plan.....	337
D Intrusion Checklist	365

Preface

Since the time the first edition of this book was published in 2000, so much has occurred in the field of computer system and network security. The Internet continues to modify and affect the way in which one does business. New national and international laws and regulations related to computers, networks, and Internet usage have been drafted, recommended, rejected, modified, and some eventually enacted. The ever-increasing progression and speed of new hacker techniques and system and network exploits have resulted in the ongoing development of a national infrastructure to deal with such issues. The world situation related to terrorism has increased the threats against our nation from a physical security perspective as well as against digital communications. The security budgets of the military, public and private industry, and government and educational sectors have significantly increased to meet the burgeoning challenges and requirements created by change over the past several years.

While security challenges have increased, so has our response to those challenges in the form of more sophisticated security technology, cooperation between consortia designed to communicate quickly and freely those effective techniques for combating security vulnerabilities, responding to incidences, and exposing hacking and attack efforts. Additionally, there is an increased appreciation and acceptance that user security awareness and cooperation are necessities. It is well-known that many successful attacks go unpublished and unqualified due to embarrassment, the need for confidentiality, and potential liability; however, the computing society has become much more willing to work cooperatively with each other to provide a force multiplier against computer security concerns.

Why is this book necessary? There is a wealth of organizations, publications, certifications, technologies, software, precautions, regulations, and procedures, all designed to guide us in becoming effective at security management. This book is necessary because security management has become an overwhelming task to first understand and then to manage, a task that feels nearly impossible to the newcomer in the field of security and a task overwhelming the already overburdened manager seasoned in security management. It is not getting any easier. The information security

field itself is reaching a stage of maturity. The security manager, however, is paralyzed by the hundreds to several thousand very specific vulnerabilities, and security management to him can appear as an insurmountable task.

This book is designed to incorporate the knowledge gained through the past decade as well as more recent methods that have pushed the security life cycle from infancy through development and now to a more mature, understandable, and manageable state. Those in the field of security who have lived through and responded to the successful attacks, disasters, and recoveries are willing to cooperate and share their experiences by developing the tools, checklists, processes, organizations, and publications to enable the computing community to stay in front of the vulnerability freight train. This book attempts to simplify security by providing understandable and organized methods and by guiding the reader to the available and most effective resources. Security management is about understanding the beast and being organized and equipped to tame it.

The original publication of this book is still valid in its approach to developing an effective Information Security Architecture (ISA). To the five original components of an ISA, however, three components (items 6 through 8 below) have been added:

1. Security organization/infrastructure
2. Security policies, standards, and procedures
3. Security baselines/risk assessments
4. Security awareness and training programs
5. Compliance
6. Monitoring and detection
7. Computer incident/emergency response
8. Disaster recovery/business continuity planning

In addition, the threat has changed. It has become larger; and with that increase, the potential losses have become more substantial. To a much greater degree, our national infrastructure is now the target. The national infrastructure includes the information infrastructure that is interrelated with a set of critical infrastructures that support our society (such as government, emergency services, water supply systems, energy, transportation, telecommunications, banking and finance, and public health).¹ A disruption to these critical infrastructures through the information infrastructure spells disaster for our nation. We rely on the information infrastructure to provide accurate and timely control of all other critical infrastructures.

Technology has changed. Organizations are implementing wireless networks with personal digital assistants capable of sending and receiving e-mail. New operating systems such as Windows XP are available; and for those on older operating systems, there is the need for research into

proper implementation. Stronger encryption methods are constantly updated to combat the threat. Research continues on new vulnerabilities and new mechanisms to control them. Once experimental, security controls such as biometrics are now becoming the standard.

Our ability to detect, react to, and recover from security incidences has changed. Technical and procedural resources are readily available. The speed and organization in which we gather, digest, and implement them are critical.

Since the original publication in 2000, organizations focused on security at that time should have gone through several iterations of the security life cycle related to their internal systems and should now be ready to advance to a more mature state of security implementation. This includes the incorporation of more sophisticated conventions and technologies such as honeypots, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), content filters, biometrics, expanded security staffs and budgets, security quality control standards, defense-in-depth implementations, development of Computer Emergency Response Teams (CERTs), forensics, investigation, business continuity, disaster recovery, and advanced security procedures. It is no longer a luxury to implement security controls; it is quickly becoming mandated for many industries supporting our National Information Infrastructure (NII) in accordance with recent governmental regulations. Hence, organizations must continue to modify and adjust their methods, efforts, and priorities by being educated, proactive, responsive, and, when necessary, reactive in the area of security management.

In addition to the components of an Information Security Architecture, this 2nd edition has been modified to provide those individuals new to the security field with a primer on general security methods. This publication has been expanded to provide the veteran security professional with an understanding of more recent legislation related to cyber-crime and information assurance, monitoring technologies such as honeypots and intrusion prevention systems (IPSs), integrated security mechanisms such as Active Directory, business continuity and disaster recovery requirements, identity theft and Internet fraud, and the latest vulnerabilities, their risks, and mitigating techniques in response.

Security is not simple. This book will help the reader understand that with a basic understanding of security principles, an analysis of an organization's computing environment, the guidance to find appropriate and effective tools for implementation in a computing and information processing environment, and a methodology for effective implementation, security can be less of a burden and a much more of an educational and enriching process.

Note

1. Defense Information System Agency, Information Age Technology, Version 2.1, July 2001.

Executive Summary

Organizational computing environments continue to evolve as the government, military, educational institutions, and public and private industries become increasingly interconnected worldwide through the information superhighway. Information technology continues to advance with the elimination of legacy mainframe systems and the maturation of distributed and multi-platform processing environments, the acquisition of new applications, and the integration of systems with Internet technology to meet ever-changing business requirements.

As it becomes easier to exchange information, it becomes more difficult to protect it. All organizations are now targets of a siege on computer systems and the information they transmit. That siege is defined as “information warfare.” The defense of this not so new but better understood threat is not only a concern for the government, military, or intelligence communities, but also for all industries and business sectors.

The government, military, and intelligence communities are aware of the interdependencies that exist in all sectors of this nation in the makeup of the National Information Infrastructure (NII). We are now interconnected worldwide through digital communications; and through those digital highways, we can be exploited somewhat simply. Technology makes this exploitation easy and at a modest cost. All that is necessary is a phone line, modem, computer, Internet connection, and a little bit of determination. It is that simple. Attackers rely on their own subculture, including private clubs, groups, newsletters, bulletin boards, and conventions where members exchange exploit techniques and information. As defenses and countermeasures are developed, hackers find ways to defeat them and publicize their efforts within their dark communities for their cohorts to continue the challenge. Attacks are concealed and can be launched thousands of miles away from their targets — as far as another country — thus making the risk to the perpetrator low.

The threats exist in varying degrees and include:

- Corporate and government insiders
- Foreign and domestic business competitors

- Intelligence agents
- Teenage hackers working silently from their bedrooms and basements

Some perpetrators pass through unauthorized systems just to view the landscape and are content simply with invading privacy. Others are malicious in their objective to electronically enter banks, business offices, governmental agencies, and homes to destroy, steal, or alter information to confuse and disrupt business or to halt operations. Successful attacks have resulted in interruptions of 911 services and air traffic control communications. These types of attacks leave no one immune.

The objectives of these perpetrators include political, economic, and financial gain. Both foreign and domestic companies and governments are willing to conduct “information warfare” in the pursuit of obtaining a competitive edge by stealing proprietary information. Other attacks are aimed at:

- Disrupting communications
- Altering or destroying databases
- Spreading misleading propaganda
- Cutting off phone services
- Stealing money
- Corrupting or deleting data
- Planting viruses, Trojan horses, worms, or time bombs
- Gaining access to sensitive data
- Selling information
- Pirating computer software

Government studies indicate that 98 percent of intrusions go undetected. Of the 2 percent that are detected, 5 percent of those get reported. These figures boil down to a mere ten incidents in 10,000 being discovered or having the potential to be addressed appropriately.¹ With so few incidences being detected and analyzed, companies find it difficult to put a price on the damage and financial loss that is incurred. The following incidences that were detected and analyzed put some perspective on the financial, political, and economic loss:

- Between 1986 and 1988, a group of foreign hackers in Hannover, West Germany, successfully accessed more than 250 systems worldwide, including U.S. military defense contractors, universities, and research organizations and 90 military sites. The theft included information, passwords, and access codes that were sold to the KGB.
- In 1989 through 1990, hackers accessed the public branch exchange (PBX), the internal phone system, of the Office of Drug Enforcement in Houston, Texas. Over a period of 18 months, these hackers used the access codes for long-distance voice and data calls. This theft resulted in the government footing a \$2 million bill in calling costs.

- In Washington, D.C., an individual used his home computer to remotely connect to the systems at the Immigration and Naturalization Department, generating immigration documentation that was sold to illegal alien clientele for \$800,000. The individual responsible was in charge of computer security for the Immigration and Naturalization Department.
- In 1994, password cracking cost telephone companies more than \$80 million in lost telephone revenues.
- In 1996, hackers broke into the Los Alamos National Laboratories in New Mexico using tools and tips they had taken from the Internet. Using a well-known UNIX loophole in an e-mail program, they were able to bypass the firewall and gain access to several of the Lab's computer systems. From these systems they attacked the super-computer center in San Diego, destroying e-mail and data files.
- Surplus computers from a U.S. attorney's office were sold at government auction. The information stored on those computers was supposedly erased. The data contained sensitive information, including the names of undercover agents, informants, and witnesses. The government learned of the incident after the sale; however, it was never determined who was potentially put at risk.

There are countless other tales of theft, loss, and destruction. It is not necessary to be a military or government organization that stores highly classified information to become a victim. Many attacks occur through automated software designed to randomly scan sequential Internet Protocol (IP) addresses and ports. Once systems have been identified as having weak computer defenses, one then becomes a target for exploitation and can be used as a launching point for other attacks or a storage site for unauthorized information gathered from a hacker's previous exploits.

The Privacy Act is yet another consideration. Although a business might process strictly unclassified information, one must protect the privacy of any information that one stores on employees, clients, or business partners. One can be held accountable for any personal information that the organization has failed to properly secure.

The National Infrastructure Protection Center (NIPC) was formed in response to the growing threat to our nation's infrastructures. The NIPC is a joint effort between the FBI, federal agencies, and private industry to prevent and respond to cyber-attacks on this infrastructure, including telecommunications, energy, transportation, banking and finance, emergency services, and government operations. The recognition that government and the private sector need to work together to bring about awareness and be more effective in thwarting the increasing cyber-crime threat provided the impetus for forming such an organization.

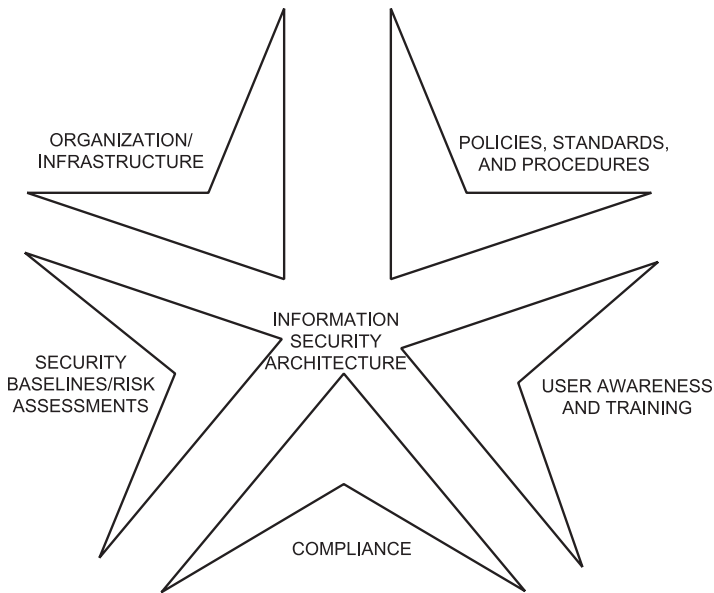


Exhibit I-1. Information Security Architecture Components

The threats are real and organizations are now starting to understand the vulnerabilities, risks, and potential losses to their information assets. Although more and more industries are increasing their security budgets, acquiring the appropriate human and financial resources to offset the growing threats to information security continues to pose a challenge to most organizations. Organizations need assistance in developing and implementing a comprehensive and flexible enterprisewide Information Security Architecture (ISA) to protect the confidentiality, integrity, and availability of their information and system resources in the ever-changing threat environment.

This book is designed to provide executives, such as the Chief Financial Officer (CFO), Chief Operating Officer (COO), Chief Executive Officer (CEO), and Chief Information Officer (CIO), with an understanding of the requirements for a strategic plan for security within the organization. It also provides the implementers of the ISA with step-by-step guidance to analyze, develop, and implement a logical and effective program that obtains the security objectives of the organization.

The first section of this book — “Information Security Architecture” — is designed to give the reader an understanding of the necessity for and requirements of an integrated plan (see Exhibit I-1). It provides a brief overview of the five components essential to an effective architecture. Those components are:

1. Security Organization / Infrastructure
2. Security policies, standards, and procedures
3. Security baselines/risk assessments
4. Security awareness and training programs
5. Compliance

These components are described in detail in Chapters 2 through 6. Each chapter provides an understanding of the component and its relationship to the other components in the architecture. It also outlines how to establish an effective plan to implement each component within the organization.

It is common for an organization to concentrate only on the current state controls within its processing environment. Usually, this is driven by a requirement for a general computer controls assessment related to the annual financial audit. General computer control assessments fall under component 3 (Security baselines/risk assessments) and can provide some indication of the strength or weakness of an organization's security program. Security baselines and general computer control assessments are often the only effort made toward establishing a security program. It is necessary to consider each of the eight components and that adequate resources are budgeted to:

- Develop an adequate security infrastructure by defining the roles and responsibilities of key personnel throughout the organization.
- Establish security policies, standards, and procedures that define control implementations, are supported by management, and adhered to by everyone in and associated with the organization.
- Identify strengths and weaknesses in the control environment of all processing platforms, databases, networks, and applications through both internal self-assessments and external reviews and make corrections to those weaknesses for continued improvement.
- Develop and implement an effective user awareness program that communicates the policies, standards, and procedures to all users and makes them aware of the risks and consequences of improper use of information and processing resources.
- Establish a mechanism to monitor the effectiveness of the security program through periodic audits and compliance testing.
- Understand the laws and regulations related to securing information in the organization's industry.
- Define and implement a plan for monitoring and detection of incidences.
- Develop a computer incident/emergency response capability.
- Identify alternate processing and operational plans for contingency purposes.

A deficiency or lack of emphasis in any one of these areas provides a weakness that can be exploited in the architecture and throughout the

organization. That is why this methodology emphasizes integration of all components and looks at each component's effect on the others.

An architecture is not difficult to establish with appropriate management emphasis, a plan, and solid organizational skills. This book outlines the step-by-step approach for establishing the ISA through an organized methodology. The security of a house is the perfect analogy to illustrate how each component of security is an integral part of the architecture and should be a consideration in increasing the effectiveness of an ISA.

A typical house contains several entryways: the front, back, and garage doors. There are typically 40 windows, each window providing an entry point into the home. When the three doors are locked but one of the 40 windows is left open, the effectiveness of the home's security system is reduced. If a window on the second floor (or secondary level) of the home is left open, but all doors and windows on the first floor are locked, a minimal deterrence exists to those who want to intrude. It will depend on how diligent or determined the intruder is, and if he wants to climb to the second floor to enter. In this example, there are levels of deterrence: locking only the doors and windows on the ground floor or additionally locking the windows on the upper floors. In the ISA, there are also levels of deterrence based on the amount of risk present in the environment and how much of that risk management is willing to accept.

The security in this house example also depends on the people who reside in the home and what is each individual's understanding of security and contribution to it (organization/infrastructure). Is the person who lives in a room responsible for locking that room's window or the doors when he leave? What has been communicated (policies and procedures) to each individual in the home to ensure that he or she knows to lock the doors and windows upon leaving? In what type of neighborhood (risk environment) is the house located? Given the level of risk, what steps can be taken (security baselines) to increase the security — a metal door, a large dog, a gated community? Have inhabitants of the home communicated to their friends where the hidden key to the front door can be found (user awareness training)? On a periodic basis, are all windows checked to ensure that the latches are in the proper locked position, or that locks are changed when the door keys have been compromised or lost (compliance)?

Now that the residents have lived in the neighborhood for five years, the neighborhood is starting to go downhill. There have been three break-ins over the past two months in which victims lost everything of value and the perpetrators were not caught. The threat of being robbed is getting higher. The residents decide that with the increasing risk, an infrared motion detection system should be installed with window and door sensors to alarm the local police if the seal is broken when the system is activated (monitoring and detection). In addition, the mother-in-law is moving in and

she is over 80 years old with a heart condition. It is decided that 911 should be added to the panic panel so that an ambulance can be dispatched in case of an emergency. On the panic panel there are also buttons to automatically alert the local police and fire station of a problem (CIRT/CERT).²

Our resident videotapes all the contents of the home to calculate its value and realizes that artwork purchased two years ago has increased in worth by 30 percent. Additional insurance is taken out on the artwork and other furnishings...just in case...(disaster recovery/business continuity planning).

A titanium front door is not going to be effective when the back door is left open or if an intruder knows where the key to the house is hidden. Weaknesses in one area can render useless the expense taken to strengthen another area, such as the titanium front door. It takes a combination of mechanisms that work in concert for security to be effective. Technology is not a substitute for the human element in fighting this threat.

There is no security solution that will guarantee that an intrusion or loss will not occur; however, levels of deterrence and detection do provide an organization with the ability to control and manage their sensitive assets and minimize losses due to both inadvertent attacks and accidental destruction. Understanding the eight components of an ISA provides a solid basis for establishing the deterrence and detection mechanisms.

Chapter 7 reviews the pitfalls and obstacles to effective implementation of an ISA. These pitfalls include the lack of a project sponsor and executive management support, the lack of understanding of risk at the executive level, the lack of resources, the effect of mergers and acquisitions on disparate systems, independent operations throughout business units, mainframe culture versus distributed computing creating the “round peg in the square hole syndrome,” the corporate culture objective to foster trust in the organization, the too rapid growth of “mom-and-pop shops” into Fortune 500 enterprises, third-party and remote network management, and the rate of change in technology. Understanding these pitfalls prior to beginning an ISA project will provide the background and knowledge to counter these issues before they manifest themselves into larger problems.

Before security technologies are implemented, a well-designed security implementation plan must be developed to ensure that the five components of an ISA have been considered and are included in that plan. Investments in technology can quickly become wasted if the infrastructure does not exist to support the maintenance of that technology. The five components of the ISA are the foundation of a secure environment (see Exhibit I-2). That foundation must be fortified with appropriate technology, methods, and programs to ensure that the information is reliable, available, and accessed appropriately on an ongoing basis.

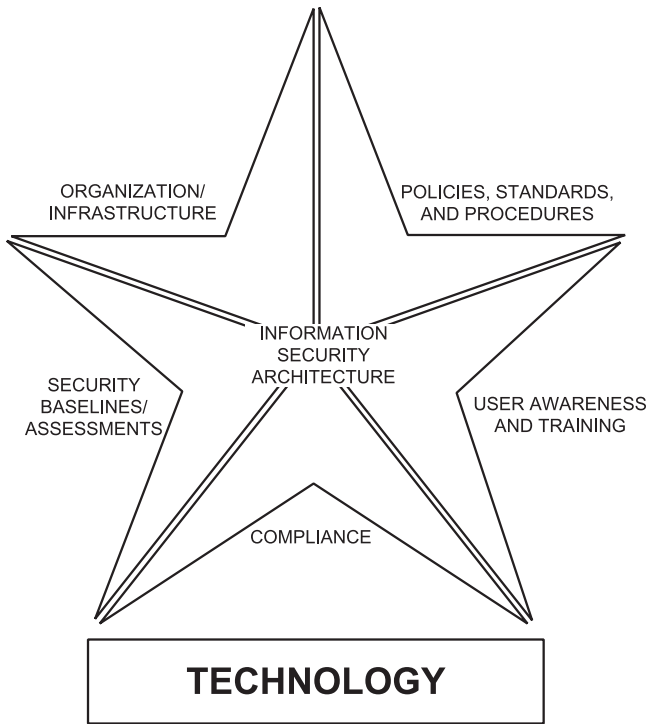


Exhibit I-2. Information Security Architecture

This book is designed to enhance the reader’s awareness of the many areas of consideration for implementing and maintaining a secure information and processing environment. Not every organization’s operating environment will parallel the situations and examples described; however, it will become clear where certain considerations for an organization will fit within the framework discussed within this book.

Look for the paragraphs that begin with the word “Incident.” These stories are true incidents that have occurred over the past several years and are either from personal experiences or have been shared between colleagues in the field of security. The incidences described are used to impress realistic risk upon the reader. So often during security assessments, it is requested from a client to list the risk along with a known security weakness. Explaining the risk has become a standard so that vulnerabilities are described in a manner that is understandable and answers the question, “What could happen if I ignore this vulnerability and do nothing about it?” Clients usually do not ignore the vulnerability by choice, but by financial constraint. One should address those weaknesses or vulnerabilities with the *most realistic* risk first.

A description of true incidents can also be used to educate decision makers on what has already occurred within their industry. Too often, resources are not allocated for the security of information systems *until* an incident has already occurred. This is known as “locking the barn door after the cows have escaped.” Describing to the Board of Directors what has occurred within their competitor’s walls is a very effective means for getting their attention as well as acquiring the appropriation of resources to ensure that the incident described does not occur in-house.

Included in each chapter is a section entitled “Getting Started.” This section summarizes the necessary steps to begin building on that particular issue or component of the ISA. You, the readers, are encouraged to use each of the workplans, templates, and guidelines as if they were your own to get your security program started. The most effective security programs are those that have active participation from within the organization. Specific expertise can be provided from outsourcing; however, the security program itself should be directed and managed internally.

Notes

1. *Networks at Risk*, Information Assurance Video Compilation I, National Command System (NCS), distributed by the Defense Information Systems Agency, May 2001.
2. Computer Incident Response Team (CIRT)/Computer Emergency Response Team (CERT).

About the Author

Jan Killmeyer is an independent consultant specializing in system and network security, enterprise security architecture development, and computer forensics. She is currently a Professor at Butler County Community College teaching computer forensics, economic crime investigation, and network security. Ms. Killmeyer is also responsible for program review of the Computer Forensics Program to ensure effectiveness and continued program development and improvement to include network forensics.

For the past 15 years, Ms. Killmeyer has specialized in the development of integrated enterprisewide security architectures for Fortune 500 companies implementing technology to obtain the strategic business objectives of those organizations. Ms. Killmeyer was the Practice Leader for Technology Risk Services in Pittsburgh and Kentucky at PricewaterhouseCoopers LLP (PwC) and the Information Security Services (ISS) group in the Information Systems Assurance and Advisory Services practice of Ernst & Young. Her responsibilities included information technology auditing, development of Enterprise Security Architecture Services, security policy, standards and procedures development, security penetration studies and risk assessments for operating systems, networks, applications and databases, internal security training program development for staff personnel, and development of the security awareness and training services for clients.

Ms. Killmeyer served 10 years of active duty in the U.S. Army as a communications engineer, specializing in tactical and strategic radio communications in Europe and classified satellite system development. She is currently a lieutenant colonel in her 23rd year of military service and is the battalion commander at the 402nd Quartermaster Battalion in the Army Reserves.

Chapter 1

Information Security Architecture

New risks and exposures accompany the widespread implementation and use of networks and a distributed client/server processing environment. Networks provide greater flexibility for accessing and sharing information and resources. The advantages to networking, however, increase the exposure of sensitive information and make it necessary to implement control strategies to maintain information integrity, confidentiality, and availability.

Security management seeks to establish controls and measures to minimize the risk of loss of information and system resources, corruption of data, disruption of access to the data, and unauthorized disclosure of information. Security management is achieved through effective policies, standards, and procedures that will ensure the confidentiality, integrity, and availability of corporate information, applications, systems, and networks for authorized users only.

Confidentiality relates to the protection of information from unauthorized access, regardless of where the information resides or how it is stored. Information that is sensitive or proprietary needs to be protected through more stringent control mechanisms. Authentication and authorization are two mechanisms used to ensure the confidentiality of information. Policies must be in place to identify what information is confidential and the period of time it should remain confidential. A framework must be developed for classifying information according to its characteristics and should include associated security requirements for each confidentiality ranking.

Integrity is the protection of information, applications, systems, and networks from intentional, unauthorized, or accidental changes. It is also important to protect the processes or programs used to manipulate data. Information should be presented to information owners and users in an accurate, complete, and timely manner. Key to achieving integrity are management controls that provide the appropriate separation of duties as well as testing and validation of any changes that are made to systems and processes. Also important are the identification and authentication of all users accessing information, applications, systems, and networks through the use of manual and automated checks. A framework needs to be developed

INFORMATION SECURITY ARCHITECTURE

for classifying the integrity of data according to its characteristics and should include associated security requirements for each integrity ranking.

Availability is the assurance that information and resources are accessible by authorized users as needed. There are two issues relative to availability: (1) denial of services caused by a lack of security controls (e.g., destruction of data or equipment or computer viruses); and (2) loss of services from information resources due to natural disasters (e.g., storms, floods, or fires). Loss of services is addressed as part of the business continuity planning process.

Chapter 2 provides a framework for classifying the confidentiality, integrity, and availability of data according to its characteristics and indicates associated security requirements for each ranking. Confidentiality, integrity, and availability together define security of information assets. One should ask the following three questions.

1. Are only the appropriate personnel viewing or using the organization's information assets?
2. Is the information correct and are the applications processing the appropriate files?
3. Are the network resources, applications, and data accessible when needed?

If the answers to these three questions are yes, it is likely that security management is being conducted effectively and the objectives of the security plan are being met. If the answers to these questions include uncertainty, this is an indication that there may be areas in the security management program that could be improved to reduce risks.

WHY AN ARCHITECTURE?

Ten to fifteen years ago, the majority of businesses operated closed processing environments. Processing platforms were proprietary and typically located in one central site and, more than likely, within a single room. Data input to the mainframe was via terminals that provided one-way communication. Computer rooms were restricted to a handful of individuals and were behind big glass windows often referred to as the "glass house."

At the advent of distributed computing, the number of processors increased while the functions performed on those processors were reduced to a specific process such as financials or inventory. The smaller processors were removed from the "glass house" and "distributed" or co-located with the business function that they supported. Communication between processors was established through networks. Users became empowered by being able to perform certain processing functions right at their desktop computers, and communication between the user and processor became two-way. A desktop user could input data and receive processed information

in the form of online reports. This decentralized processing brought the advantages of not having to rely on a single computer center for support and freed the users and departments to do some of the processing work and support themselves and getting the information that they required.

The “glass house” provided limited and controlled access to information and sensitive processing programs and resources. The move to distributed computing brought greater empowerment and increased efficiency to the users but opened up a multitude of control issues that need to be considered and addressed when moving to this type of processing environment. In the days of centralized processing and mainframes, information security was the responsibility of one individual — the mainframe security officer. Now, information security touches everyone within the organization.

As desktop and laptop PCs are handed out to each employee, each employee has a responsibility and commitment to maintaining the confidentiality, integrity, and availability of the information to which he or she has access. An integrated information security architecture (ISA) is the mechanism to ensure that all individuals know what they are responsible for and how they need to go about protecting those resources.

Information security risks are on the rise. Incidences of viruses, hackers, theft, sabotage, and corporate espionage are being publicized much more frequently, and corporate management has become more eager to listen. The media has played a key role in educating decision makers on the risks of open systems, and those with decision-making ability are becoming much more interested in *not* becoming a statistic in the information security headlines. Too often, however, decision makers react only after they have become a victim of a security incident.

INCIDENT. During a network security assessment project for a major national bank, the assessment team cautioned the bank on the installation and configuration of a new firewall system that was being implemented for access to the Internet. It appeared that the individual in charge of the project was choosing the firewall vendor based on what had been implemented at his previous place of employment. Appropriate requirements definition, system selection procedures, and analysis of the effectiveness of the firewall products currently available on the market had not been performed. The assessment team’s firm had previously and independently performed a systematic evaluation of the top firewall vendors on the market. The bank’s selected product had not fared well when compared to the independent firewall evaluation.

During the first several months of the project, the team had been unable to meet with the individuals responsible for both the firewall installation and the separate “secure” segmented network on which the firewall was to be installed. This network operated independently of the rest of the bank’s

INFORMATION SECURITY ARCHITECTURE

network resources and had its own network management personnel to manage this segment of the network. Several months into the project, the manager of the firewall reported that there was a curious outbound file in the queue that was being transferred to someone on the Internet. Somehow, the file had gotten stuck and had not been transferred. Further investigation showed that the file was the bank's UNIX password file on its way out the door of the network to an unknown destination. Shortly after the incident, the project manager was sitting in the independent assessment team's office asking for advice and more than willing to talk about appropriate configuration management and the soundness of their router access control lists.

The real issue with this story is that it is unknown how many other system password files had already been transferred and what the previous or current damages were that had occurred related to breaches of confidentiality, unauthorized access, and changes to system and data files. This organization had no incident response plan to assess the damage or to quickly secure or shut down the processes under attack.

Another key risk, as demonstrated by this story, is that management often feels that because they have invested in a security solution, such as the firewall, they have done enough to protect themselves. The most significant risk in this case is that incomplete defenses or solutions provide a false sense of security.

To gain an understanding of how this security incident and the firewall solution could be implemented more effectively, one can analyze the solution relative to the five components of the ISA. First, when the bank bought the firewall, did it have qualified personnel to implement it and were enough human resources allocated to provide daily monitoring and maintenance of the system? The individual responsible for the firewall product should have been identified in the security organization and infrastructure. Typically, this individual becomes the application owner. The roles and responsibilities of this individual should be documented in the individual's job book and appropriate time budgets prepared for each responsibility related to the security role. When implementing new technology or applications, estimates of time budgets often have to be readjusted once the technology or application has been installed and is operational. Adjustments to resource requirements can be made in the next fiscal year or immediately if resources are available.

Second, the application owner needs to understand what is defined as appropriate operation. Policies, standards, and procedures need to be specifically developed for firewall operation. This documentation will address:

- Who is permitted to use the application
- What types of services will be provided by the system
- How users will request access to the system

- Who will grant access to the system
- How often access logs will be reviewed
- What procedures will be taken for inappropriate use of the system
- How security incidences will be reported, recorded, and handled
- Who will be responsible for investigating suspicious activity

Usually, this type of documentation does not get discussed or written down until a situation occurs that requires these questions to be answered. Often that is after a security violation or incident has occurred.

Third, the firewall configuration needs to be tested. It should already be clear what the security objectives and capabilities are of the firewall. The vulnerabilities of the system should be reviewed and known. Once the configuration is complete, an attempt to thwart the system should be performed so that both the capabilities and weaknesses are known, documented, and improved. This is called *baselining the security of the system*. In the case of firewalls, automated software exists that tests the configuration for known vulnerabilities. This automated software is frequently updated to include the most recently identified software changes and new tests for operating system vulnerabilities.

In the security industry today, as soon as a product is developed, hackers quickly discover how it can be broken and what are the loopholes and weaknesses. As the loopholes and weaknesses are discovered, new compensating controls must be implemented. That is what makes the security industry so dynamic. There are many brilliant minds out there waiting to be challenged. It is not acceptable to purchase a product, configure it, and let it sit there by itself, with the thought that it is performing its function effectively. It must be constantly monitored and reconfigured to meet the new risks and vulnerabilities that are continuously exposed. It is one thing to purchase a product and another to implement it properly and provide appropriate budget and resources to operate the product effectively. The product must also be integrated into other compensating security solutions.

Fourth, all users of the system must be made aware of what they can and cannot do by receiving security awareness training. The firewall manager must understand what executive management has in mind for the use of the Internet access and the firewall, what services will be provided on the Internet, and based on those services, properly configure the hardware and software. Users of the Internet must be made aware of those services they are permitted to use, such as e-mail, Web searching, file transfer, or telnet access to systems on the local network or distant systems. It needs to be made clear what the consequences will be if the policies related to the Internet are not followed. In the case of e-mail services, soliciting for your child's school fund-raiser through e-mail messages is commonly prohibited because it is nonproductive, annoying, and could

walk the line of harassment in work relationships. Accessing sexually explicit Web sites at work locations is also a common item that is restricted for similar reasons. Employees should also be made aware that conducting personal business through e-mail is prohibited. If an organization fails to make these restrictions known to its employees, management will be unable to enforce its policies.

Finally, procedures need to be established to ensure that all parties responsible for the Internet access and firewall configuration are in compliance with the security policy, standards, and procedures that have been developed, and that the programs developed to enforce the policies are effective. One-time compliance checks will not do the trick. Compliance is a cyclical check that, depending on the level of risk, needs to be performed either daily, weekly, monthly, quarterly, or annually. Compliance programs should be designed to measure the effectiveness of the integrated security plan implementation efforts. Chapter 6 details who is responsible for those compliance checks and how often they should be performed. In the case of Internet access, reviewing firewall logs for access attempts should be performed daily by the component owner. Scanning the firewall with automated software to test for weaknesses in the configuration is more than likely a monthly or quarterly event performed by internal audit, the component owner, or outsourced to a security consulting firm, depending on the level of expertise that exists within the organization.

It should now become clear how eliminating any one of the considerations outlined in this example would provide weaknesses in the Internet access and cause considerable vulnerabilities to the entire organization's processing environment. Each of the organization's components — operating systems, databases, networks, access points, and applications — should be analyzed according to the components of the ISA to ensure that all security considerations have been made for that component. As with a house, leaving a single window open on the ground level of one's home will reduce or negate the efforts made to secure the rest of the home. An integrated approach to security in the operating environments of today's organizations is not an option — but an absolute necessity.

Client/Server Environments

Client/server technology has moved information technology (IT) systems from closed to open processing environments. According to *Newton's Telecom Dictionary*, client/server is defined as “a computer on a local area network from which you can request information or applications.”

The original meaning of the term refers to you — the user — as the client and the computer as the server. The meaning of client/server has evolved and now refers to a computing system that splits the workload between

PCs and one or more larger computers on a network. In most cases, the “client” is a desktop computing device or program “served” by another networked computing device. Computers are integrated over the network by an application that provides a single system image.

Storing and processing sensitive information at the user location and transmitting it across networks results in control issues that need to be addressed within the ISA. What is meant by closed versus open processing environments?

- **Closed¹:** – Traditional IT systems and networks are closed. Only named parties can send messages. The nodes and links are known in advance. The insertion of new ones requires the anticipation and cooperation of others. They are closed in the sense that their uses or applications are determined in advance by their design, and late changes are resisted.
- **Open²:** – By contrast, modern computing environments are open. Like the postal system, for the price of a stamp anyone can send a message. For the price of an accommodation address, anyone can get an answer back. For not much more, anyone can open his own post office. Modern networks are open in the sense that nodes can be added later and without the permission or cooperation of others. They are open in the sense that their applications are not predetermined.

If sensitive information is processed in a distributed fashion and transferred over networks, those with potential access to that information would be anyone who has access to the network. Closed processing environments limit access to known nodes and users on the network. Open processing environments expand that access to anyone who can send or receive information via that network. This includes essentially anyone who can easily establish an address and send and receive to a node on the internal network.

Why would anyone want to implement a processing environment that poses control issues? Simply because there are many advantages that outweigh the costs of not implementing it. The advantages of client/server are:

- Users can do their jobs more efficiently by decreasing processing response time and application development time.
- Users can obtain the information they need more quickly and without having to request it through a third party.
- There is transparent access to shared data and more efficient use of existing resources with the emergence of access enabling tools.
- Graphical user interfaces (GUI) are a by-product of client/server technology and enhance productivity because they are much easier to use than the traditional character user interfaces of traditional mainframe systems.

INFORMATION SECURITY ARCHITECTURE

- Adding processing and storage resources as the production environment grows is easier, cheaper, and increases the life of the technology investment.

The disadvantages of the client/server environment must be weighed prior to implementation. If an organization is unable, from a management and financial standpoint, to address the control issues related to the client/server environment, then it should not implement client/server technologies. The disadvantages of client/server are:

- Client/server relies on networking between different types of networks, or internetworking. Internetworking management products do not support all network protocols and may require the purchase of several internetworking management products. This can increase the cost of maintaining client/server systems.
- Because the technology has only been introduced within the past decade, client/server applications and software tools have not matured. The software and applications are still being modified to meet security, internetworking, and user requirements.
- Software distribution and configuration management is more difficult in a distributed environment than in the traditional mainframe environment.
- Multiple databases exist in the client/server environment, requiring the management responsibility of synchronizing data shared between clients and servers.

Regardless of the advantages and disadvantages, the majority of organizations are migrating from traditional mainframe environments to the distributed client/server architecture. Networking in an open system environment, specifically internetworking, poses security and control issues related to the confidentiality, integrity, and availability of the information transmitted across these networks. *Newton's Telecom Dictionary* defines internetworking as "communication between two networks or two types of networks or end equipment."

This may or may not involve a difference in signaling or protocol elements supported. In the narrower sense, it is to join local area networks together to enable users to get access to other files, databases, and applications. Bridges and routers are the devices that typically accomplish the task of joining LANs.

Internetworking is concerned with more global telecommunications issues that include heterogeneous, multi-protocol, bridge- and router-based topologies. Under traditional networking concepts, this creates a relatively open and unprotected environment. Understanding each of the components of the network and processing environment and implementing control policies and procedures for each of these components minimizes

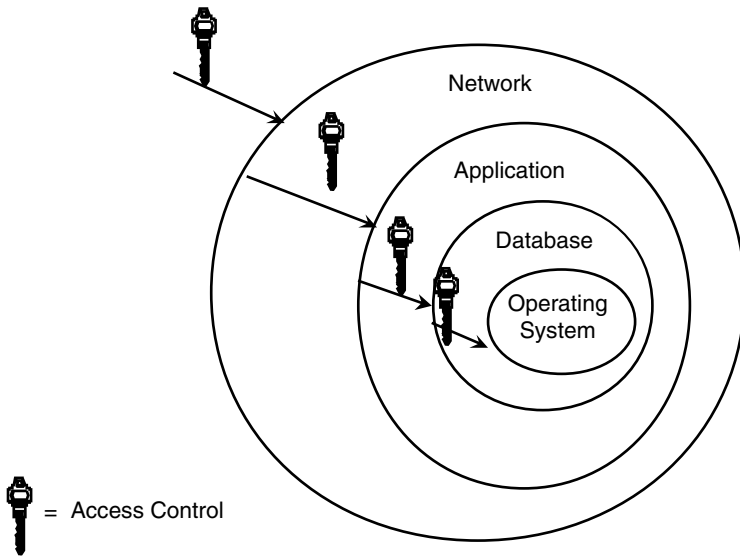


Exhibit 1-1. Layered access controls.

the risk of unauthorized use and manipulation. The bottom line is that more people have access to more processing resources, applications, files, and information. Protecting the confidentiality, integrity, and availability of those assets becomes a significant control issue.

The ISA takes into consideration each of the access points into the organization's network. If unauthorized access to the network can be controlled, unauthorized access to components on that network is minimized related to external threat. One's network is the front door to one's operating environment. Once an intruder has entered the front door, he can go up to each of the bedroom doors and attempt to enter. Protecting the front door is critical to protecting each of the subsequent layers of the operating environment (see Exhibit 1-1).

In traditional operating environments (mainframe), the emphasis was placed on the application or access to the mainframe itself. In a distributed environment, this emphasis must shift to the first line of defense, the network. Access points in today's networks include remote node access, dial-in and dial-out service, electronic funds transfer (EFT), bulletin boards, inter-departmental electronic mail, electronic data interchange (EDI), local area networks (LANs), wide area networks (WANs), and Internet (see Exhibit 1-2).

Communications networks have become the system that binds information and users. The fast pace of change in communications technology has

INFORMATION SECURITY ARCHITECTURE

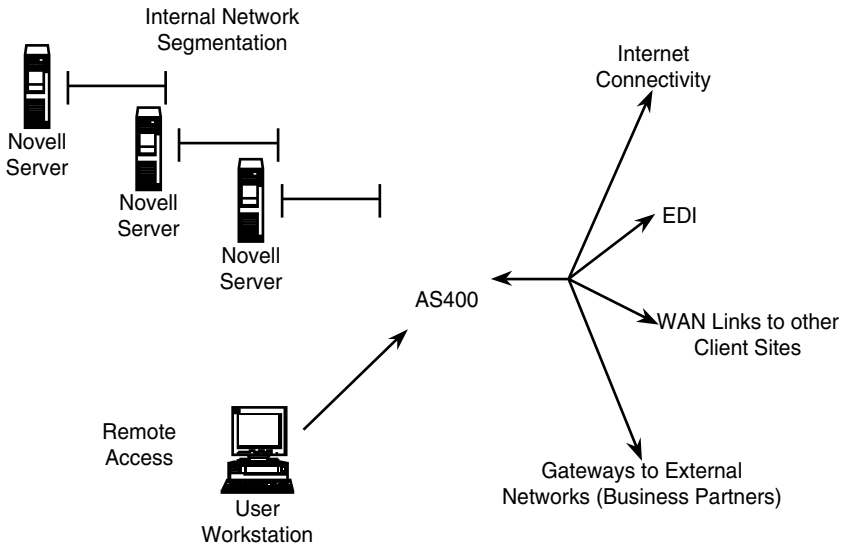


Exhibit 1-2. Potential network access points.

caused IS organizations to piecemeal their communications requirements as well as their security practices, creating an unmanageable and risk-affinitive environment. What is meant by piecemealing? As an organization grows, the tendency is to add to the existing environment to meet current requirements without planning for future growth. This can occur due to lack of knowledge on available technology, lack of communication between departments, or nonexistent technology standards within the organization. For example, some organizations allow individual departments to decide on their communications architectures. This author has seen organizations that have three different local area network (LAN) architectures: Novell, Windows NT, and Banyan Vines. If all of the departments are relatively independent, do not share data, and have enough resources to support the management of three different network operating systems, this might be a viable option. In this particular organization, the decision to allow each department its own freedom in choosing, implementing, and maintaining processing technology eventually became cost-prohibitive. The necessity to share data and the popularity of e-mail became a technological problem because of the lack of standards between departments. Eventually, this organization decided to reduce costs by moving the technology support personnel from the departments to a centralized help desk, and to establish software and hardware standards to minimize the number of operating systems, applications, and equipment that would require support.

In over half of the network assessments performed, this author identified to the client organization access points in the operating environment

of which the organization was not aware. This does not mean that someone was not aware of them, only that the information systems department or persons responsible for authorizing access were not aware that a path to or from their network had been established. One may be curious as to how and why the responsible individuals were not aware that these access points had been established on their network. The simple answer is that effective controls were not in place — controls such as procedures for authorization of the access point, policies providing guidance on the appropriate use of desktop modems, or user awareness training that communicated to the departments and users what they were allowed to do and not allowed to do with their processing resources. Another reason is simply that departments within the organization failed to communicate their requirements with each other. In the case of one large bank, the information technology department conducting a network assessment study was unaware that the bank was paying five different Internet service providers (ISPs) for Internet access throughout the bank. Mergers and acquisitions played a role in this situation, but nonetheless, all of the departments were on one network. A single access point to the Internet could have been established producing a central point of administration as well as economies of scale in cost when dealing with a single ISP. Assessing the network and risks related to access points on the network is discussed in further detail in Chapter 4, Security Baselines and Risk Assessments.

Overview of Security Controls

Security includes confidentiality, integrity, and availability. A secure processing environment includes making sure that only those who are authorized have access to sensitive information, that the information is processed correctly, and that it is available when necessary.

To apply appropriate controls to an operating environment, it is necessary to understand who or what poses a threat to the processing environment and then to understand what could happen (risk or danger) from that threat. When the risk is understood, management must decide what it wants to do about that risk. Management can accept the risk as it has been assessed and understood, or do something to reduce the risk to an acceptable level. This is known as risk mitigation or risk reduction. The third choice management has is to transfer the risk; that is, buy insurance. This provides no preventive measure for undesirable situations, but does provide some degree of compensation for a loss. This book concentrates on management's second choice — risk mitigation or risk reduction by implementing effective controls.

The Threat. Corporate information can be easily accessed, compromised, or destroyed by intentional, unintentional, or natural threats. Intentional threats are unauthorized users who inappropriately access data and

INFORMATION SECURITY ARCHITECTURE

information that they are not granted permission to view or use. These unauthorized users can be external or internal to the organization and can be classified as curious or malicious. The curious will usually just look around and are not always sure of their own intentions or of what they will find. The malicious have intent to steal out of profit motive or to destroy resources out of revenge. Unauthorized access of curious users typically results in a breach of confidentiality and sometimes integrity if they are not sure of what they are doing. Intrusion by malicious unauthorized users first results in a breach of confidentiality, leading to breaches in integrity and, possibly, availability.

Unintentional threats are typically caused by untrained or careless employees who have not taken the steps to ensure that their passwords are protected, their computers are properly secured, or that virus scanning software is frequently updated and executed on schedule. Unintentional threats also include programmers or data processing personnel who do not follow defined standards and procedures designed to build controls into the operating environment. This threat exists in environments where no defined standards or operating procedures exist. An example of this is the programmer who has access to executable files and programs and makes changes to those programs in the operational environment instead of a test environment. Simple mistakes in a program can affect the integrity of the entire application and any integrated applications using common information.

Natural threats include equipment failures, or disasters such as fire, floods, and earthquakes that can result in the loss of equipment and data. Natural threats usually affect the availability of processing resources and information. Exhibit 1-3 outlines the most common concern for each type of threat and its result.

The Risks. There are many events that can result if a breach of confidentiality, integrity, or availability occurs. From a business standpoint, there is almost always financial loss involved. The business risks include contractual liability, financial misstatement, increased costs, loss of assets, lost business, and public embarrassment.

INCIDENT. A famous entertainer was in town for a performance and suddenly was taken ill. Unable to be attended by her own physicians due to the emergency, she went to a local hospital, was treated and released. A system user at the hospital obtained the entertainer's record of treatment and released it to the newspapers. The entertainer sued the hospital for an undisclosed amount and settled the lawsuit out of court. Although the settlement amount is not known, this entertainer was quite famous and worth a nice fortune. It is doubtful that she sued for just thousands of dollars. This author would venture to guess that the settlement was upward of several million dollars. This is a significant sum to pay for a single breach of confidentiality.

Exhibit 1-3. Threat/Concern/Risk Matrix

Threat	Concern	Risk (Event)
Unauthorized user (curious) → →	Confidentiality → → Integrity	Unauthorized access Unauthorized disclosure Unauthorized observation Unauthorized monitoring Unauthorized copying Stealing
Unauthorized user (malicious) → →	Confidentiality Integrity → → Availability	Enter, use, or produce false data Modify or replace valid data Misrepresentation or repudiation Misuse of data Failure to use data/resources as required
Authorized user → →	Integrity Availability → →	Destroy, damage, or contaminate Deny, prolong, or delay use or access
Natural disaster → →	Availability	

As a result, this hospital then conducted a risk assessment to determine what needed to be done to prevent similar situations from occurring.

An example of the effect financial misstatement can have on an organization is similar to the effect seen on the stock market when quarterly earnings are posted on publicly traded stocks. Earnings that do not meet the earnings estimates lose value on the market. Public accounting firms are responsible for ensuring that publicly traded companies have appropriate and effective management controls as well as general computer controls in their operating environment. Public accounting firms are also responsible for ensuring that the financial statement accurately reflects the health of the organization. Financial misstatement or errors in accounting that are material can have the same effect in plummeting the value of stock when the errors are discovered. Stock owners lose confidence in the leadership of the organization and will immediately sell their shares to minimize their losses.

Increased costs occur from many types of security incidences. A lack of integrity in systems and data will result in significant cost to find the problem and fix it. This could be from having to modify, test, and install new programs or to rebuilding systems. Increased costs can also occur from hardware failures or disasters such as fire, flood, tornado, hurricane, or earthquake, in which entire systems and data need to be replaced. In the case where there is no disaster recovery plan or backup systems and data, organizations may go out of business. Viruses, once inside an organization's

INFORMATION SECURITY ARCHITECTURE

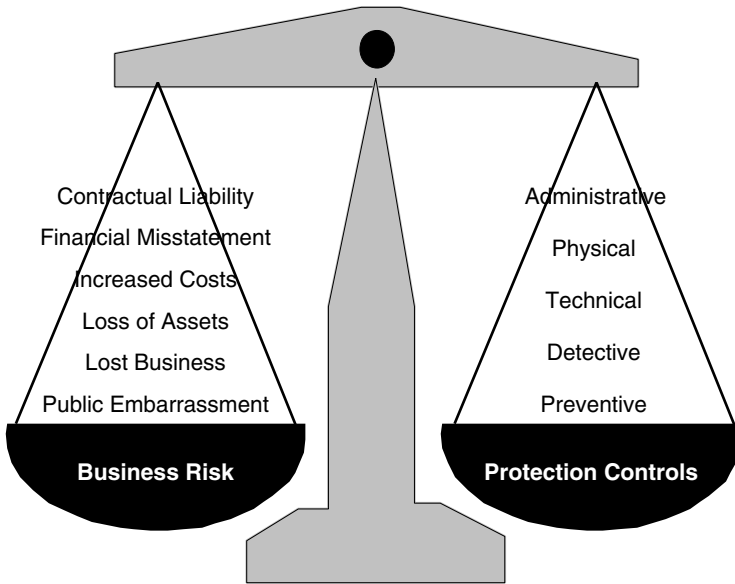


Exhibit 1-4. Risk versus controls implementation.

operating environment, can take many man-hours to fix. The cost to an organization that has had proprietary formulas, research, client lists, or strategic business plans stolen as a result of corporate espionage, may also suffer increased costs due to competition or lost business.

Public embarrassment when a security incident has been publicized or from highly visible lawsuits, such as the case of the famous entertainer, will cause a loss of business due to lack of confidence in the organization. Whatever the risk, it must be weighed and appropriate controls relative to realistic risk must be implemented (see Exhibit 1-4).

The Controls. Studies over the past several years have shown that over 80 percent of organizations have suffered some type of information or hardware loss, with inadvertent errors and viruses listed as the most frequent cause. Today, it is unheard of to have PCs or servers that do not have virus protection software. An increase in computer crime is causing IT professionals to look again at their control mechanisms. Computer crime has become a greater risk due to more individuals becoming computer savvy, having access to computing resources and the interconnection between internal and external networks. One thing is known: the majority of incidents are internal to the organization, whether they are inadvertent or malicious.

Control requirements are not uniform for all systems. The extent of business risk should determine what level of control is appropriate. Each threat

can be addressed by applying one or more security controls. Controls fall into three major categories: administrative, physical, and technical.

Administrative controls include security policies and procedures. Policies tell users what they can and cannot do while using corporate computing resources. They also include procedures for management review of changes to code, authorization for access to resources and periodic review and validation that access is still appropriate, separation of duties, security awareness and technical training, IT management and supervision, and disaster recovery and contingency plans. Administrative controls also include security review and audit reporting used to identify if users are adhering to policies and procedures. Finally, administrative controls include data/resource ownership. Security responsibility for each component of the operating environment must be defined by each individual and those responsibilities must be written into the individual's job book in order that they get credit for the responsibility as well as an evaluation on the fulfillment of their duties.

Physical controls constrain direct physical access to equipment. Physical controls consist of cipher locks, keypads, keyboard locks, security guards, alarms, and environmental systems for water, fire, and smoke detection. Physical controls also consist of system backups and backup power such as batteries and uninterrupted power supply (UPS).

Technical controls are controls implemented through hardware or software that are typically difficult to defeat and, once implemented, can work without human intervention. They are sometimes referred to as logical controls. Specific software includes anti-virus, digital signatures, encryption, library control software, network management tools, passwords, smart cards, encryption, dial-up access control, callback systems, audit trails, and intrusion-detection expert systems.

Access controls protect against unauthorized use or manipulation of resources through authentication and authorization. Authentication provides assurance of the identity of the user or system requesting access. Authorization controls ensure that access to information and processing resources is restricted based on management direction. Another term related to security is nonrepudiation. Nonrepudiation protects against one party to a communication exchange later falsely denying that the exchange occurred. The technical control used to protect against nonrepudiation is digital signature. Business transactions performed over intranets and the Internet have become commonplace. Where once handwritten signatures were used to verify that a purchase had been made or a particular contract had been agreed upon, one now has a digital alternative to verify that one will stand behind a transaction. A digital signature consists of a private key that only the key holder knows or is able to replicate, similar to his or her

INFORMATION SECURITY ARCHITECTURE

Exhibit 1-5. Information Security Controls

Physical Controls	
Preventive: Backup files and documentation Fences Security guards Badge systems Locks and keys Cipher locks/keypads Backup power Biometric access controls Site selection Fire extinguishers Keyboard locks	Detective: Motion detectors Smoke and fire detectors Closed-circuit television monitoring Sensors and alarms
Administrative Controls	
Preventive: Security awareness and technical training Separation of duties Procedures for recruiting and terminating employees Security policies and procedures Management and supervision Disaster recovery and contingency plans User registration for computer access Data/resource ownership	Detective: Security reviews and audits Performance evaluations Required vacations Background investigations Rotation of duties
Technical Controls	
Preventive: Access control software Antivirus software Library control systems Passwords Smart cards Encryption Dial-up access controls and callback systems	Detective: Audit trails Intrusion-detection expert systems

written name. Digital signatures verify the source, authenticity, and integrity of electronic messages.

Administrative, physical, and technical controls can be further subdivided as preventive or detective. Preventive controls attempt to avoid the occurrence of unwanted events, whereas detective controls attempt to identify unwanted events after they occur. It is always best to prevent a security event than to have to deal with it after the fact. When an event does occur, detective controls are designed to catch the problem quickly enough to minimize the damage and to be able to accurately assess the magnitude of the

damage caused by the incident. Exhibit 1-5³ lists the specific administrative, physical, and technical controls and further categorizes them into preventative or detective mechanisms.

Administrative, physical, and technical controls must be used collectively to meet the challenges of realistic risk in the processing environment. Management has to decide what to reasonably invest for security and control in IT and how to balance risk and control investment. As organizations restructure and streamline themselves to compete in the global economy, it is imperative that IT be used for competitive advantage. The next section focuses on IT's contribution to the organization's business objectives through the use of new technology. The Strategic IT Plan is the document used to determine how IT will support the business objectives of the organization while providing a framework for control to safeguard these assets and to manage the new risks.

The Strategic Information Technology (IT) Plan

It is necessary to point out that some organizations use the term information systems (IS) department to describe their systems function. Other organizations use the term information technology (IT) or IT department to describe the same function. Yet other organizations have both an IS department and an IT department. Typically, these organizations separate their systems department from the process of selection and implementation of new technology. This does not mean that the new technology is not considered a system. But until it has been implemented, it is part of the developmental process and most likely requires significant resources and increased attention to ensure success. Technology implementation projects tend to be split from the day-to-day operation and maintenance budget of the IS department. Companies are neither right nor wrong in how they choose to term their departments or functions. It can be indicative, however, of how large an organization's IS function is and how detailed the organization is in subdividing roles and responsibilities in the IS organization. Both terms, IS department and IT department, will be used interchangeably throughout this book.

Ten year ago, many organizations were happy not to hear or see anyone from the IS department. That was because when they did, it usually meant something was wrong or something needed to be fixed. Transparency was key and as long as IS kept everything running smoothly and stayed out of the way, all was right with the world. The IS department was viewed as a necessary evil, a support function, key but not crucial to the business. This has changed. With the client portion of client/server sitting on most employee desktops, hearing and seeing IS professionals has become a daily occurrence. Through the use of technology, the IS department has become the center of operations and key to the success of the business. Technology is

INFORMATION SECURITY ARCHITECTURE

viewed as the vehicle to achieving business objectives of increased revenue growth, production and performance, or decreasing costs. The IS department has become the means to the end through the use of technology.

The leading technologies that provide businesses with the capability to meet their business objectives are image processing, electronic data interchange (EDI), electronic commerce, communications technologies, workflow technology, area networks, collaborative computing and groupware, cooperative and client/server computing, intelligent agents, business process reengineering (BPR), mail technology, security, expert systems, quick response (QR), and telecommuting. Technology implementations are costly and many implementations have failed because appropriate planning was either not performed or was not thorough.

The business plan is the basis for the organization's existence and includes a mission statement. This statement defines the business goals and objectives that typically include references to revenue growth, increased production and performance, competitive advantage, increased quality and service levels, and decreased costs and time-to-market.

The business plan should also include a section on how the organization intends to achieve its goals and objectives. If it is through the implementation of technology, the business plan should refer specifically to the Strategic IT Plan. The business plan answers the who, what, where, when, why, and how of the business. This includes a budget for operations with a line item for the IS department. The organization may choose to break out a separate line item to support the purchase, implementation, and maintenance of new technologies.

The Strategic IT Plan supports the business objectives as stated in the business plan. At a minimum, the Strategic IT Plan should be broken into six parts:

1. Introduction
2. Description of the IT Organization
3. Scope, Viability, and Modification of the Plan
4. Relationship to the Organization's Strategic Business Plan
5. Strategic Goals for Information Technology
6. Summary and Conclusion

Section 1, Introduction, is an overview or executive summary that describes the background, origination, and intent of the document. Section 2, Description of the IT Organization, should include a definition of the roles and responsibilities of individuals within the IS department, an organization chart and description of supporting staff, and a vision for the use of IT.

Section 3, Scope, Viability, and Modification of the Plan, defines the scope of the document. An example of this section follows:

All information technology systems will be discussed, including information technology planned, developed, operated, and supported by the organization. The major goals and initiatives recommended by this plan are strategically significant to all business units of the organization. However, this document is intended to only reflect major institutional directions initially, with subsequent addition and modification to include corresponding plans of respective business units within the organization.

This strategic information technology plan is intended to be a “living” document, with the primary purpose to serve as a communication vehicle across the institution. Strategic plans typically cover a time period of five years. Changes in technology occur so rapidly that it is not realistic for this document to remain static for that time period. Consequently, this document provides the baseline for IT planning and will be modified to reflect current priorities for information technology within the organization.

At its initial adoption, this plan will consist essentially of the primary goals, or initiatives, recommended and adopted at the institutional level. In the upcoming year, a more detailed action plan will be developed within the appropriate advisory groups and management levels for specifying how strategic institutional initiatives will be undertaken. On an annual basis, a revised information technology strategic plan will be presented to the executive management for review, along with a summary assessment from the CIO of how the organization is progressing in achieving goals or undertaking initiatives indicated in the plan.

As this example indicates, the Strategic IT Plan is a document to reflect the direction for IT within the business. Supporting plans that address each technology issue should be developed in detail and include planning for cost, selection, implementation, testing, maintenance, and consideration for security and control.

Section 4, Relationship to the Organization’s Strategic Business Plan, refers back to the business plan and provides a discussion of how the plan is integrated with and supports the Strategic Business Plan. This section can also include a discussion of the industry’s direction related to IT, including competition and the industry leader’s use of technology to gain competitive advantage.

Section 5, Strategic Goals for Information Technology, lists the specific objectives from the business plan that relate to IT. A sample table of contents from a Strategic IT Plan is shown in Exhibit 1-6. It lists the business objectives as information accessibility, technology-enabled management, staff and business partners, technology-enhanced business, business process effectiveness, and information security architecture. Subsections under each IT goal describe what must be accomplished to successfully meet the IT business objective.

INFORMATION SECURITY ARCHITECTURE

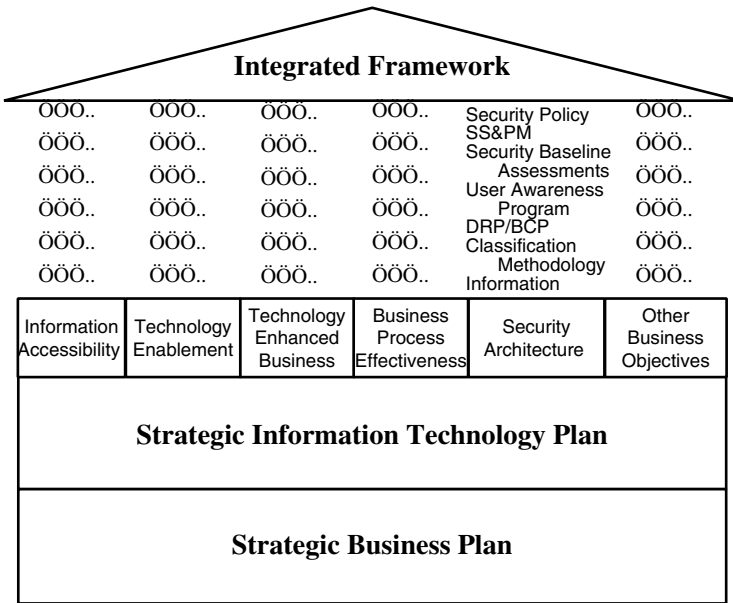


Exhibit 1-6. An integrated framework.

Section 6, Summary and Conclusion, provides a link to the specific and detailed plans that will support the Strategic IT Plan. For the information security architecture business objective, this will result in an information security architecture document that describes the five components of the architecture and includes a security policy, a security standards and procedures manual (SS&PM), security baseline assessments, a user awareness program, a compliance program, a disaster recovery/business continuity plan (DRP/BCP), and a classification methodology.

The documents shown in Exhibit 1-7 are an integrated framework for achieving the goals and objectives of the business. The Strategic Business Plan is the foundation. It lists the goals and objectives for success in the business. The Strategic IT Plan supports the Strategic Business Plan by describing how technology will be used to enhance the business. Supporting and detailed plans for each business objective, including IT business objectives, define the step-by-step procedures for bringing the business to greater levels of success. An integrated framework provides the necessary links between the business goals and objectives, ideas, and plans to achieve those objectives, and the step-by-step approach to accomplish the mission of the business.

The Strategic IT Plan needs to include the ISA as one of its objectives for the organization to operate effectively in a risk-reduced environment.

Exhibit 1-7. Strategic IT Plan: Sample Table of Contents

Table of Contents

1. Introduction
 2. Information Technology at XXXX Organization (Mission Statement)
 - 2.1 The CIO and Information Systems & Technology Roles
 - 2.2 The Information Systems & Technology Institutional-Level Organization
 - 2.3 Local Information Technology Support Staff
 - 2.4 The Evolving Information Technology Support Role
 - 2.5 A Vision for Information Technology Effectiveness
 3. Scope, Viability, and Modification of This Plan
 4. Relationship to the XXXX Corporation's Strategic Plan
 5. Strategic Goals for Information Technology
 - 5.1 A Corporate Goal: Information Accessibility
 - 5.1.1 Enhance and Extend the Network Infrastructure
 - 5.1.2 Ensure Appropriate Off-Site Network Access
 - 5.1.3 Ensure Effective Delivery of Information Technology Support
 - 5.1.4 Evaluate Services and Customer Satisfaction
 - 5.1.5 Establish Corporatewide Standards
 - 5.1.6 Effectively Manage and Distribute Servers
 - 5.1.7 Enhance Support of Library Initiatives
 - 5.1.8 Enhance Internal and External Communications
 - 5.2 A Corporate Goal: Technology-Enabled Management, Staff, and Business Partners
 - 5.2.1 Ensure Management and Staff Development in Technology
 - 5.2.2 Provide Appropriate Workstation Support for Management and Staff
 - 5.2.3 Promote Effective Research Computing
 - 5.2.4 Foster Technology Experimentation
 - 5.2.5 Provide Effective Information Technology Services for Clients
 - 5.3 A Corporate Goal: Technology-Enhanced Business
 - 5.3.1 Establish Appropriate Levels of Technology in Business Operations
 - 5.3.2 Ensure Availability of Information Technology Resources for Employees
 - 5.3.3 Engage the Corporate Community in the Use of Technology
 - 5.4 A Corporate Goal: Business Process Effectiveness
 - 5.4.1 Improve Efficiency of Operations
 - 5.4.2 Establish an Effective Data Warehouse System
 - 5.4.3 Replace Business-Process Software Systems
 - 5.5 A Corporate Goal: Information Security Architecture
 - 5.5.1 Establish an Organization that Supports the Security Function
 - 5.5.2 Establish Security Policies and Procedures
 - 5.5.3 Conduct Baseline Risk Assessments for Each Component of the Operating Environment
 - 5.5.4 Develop a User Awareness Program and Conduct Training for Employees and Individuals with Security Responsibility
 - 5.5.5 Develop a Comprehensive Compliance Program
 6. Summary and Conclusion
-

Without an ISA, the organization may go on for several years without an incident. When one does occur, however, the cost to the business could be much greater than the time and resources it takes to understand the risks, the operating environment, and the controls necessary to provide

INFORMATION SECURITY ARCHITECTURE

assurance that information, systems, and network resources are processing correctly, are safe from unauthorized use or access, and are available when needed.

SUMMARY

This chapter provides an understanding of the objectives of security, which are to ensure the confidentiality, integrity, and availability of information and computing resources through an integrated ISA. The ISA is necessary in today's distributed processing environments in which everyone inside and associated with the organization plays a role in security. The controls that are implemented include a combination of administrative, physical, and technical procedures that are chosen based on the types of threats and realistic risk that exist related to the organization's industry, market presence, and the technologies that have been implemented throughout the organization. The Strategic IT Plan is the source document that brings security to the forefront through executive leadership and is integrated with the goals and objectives of the Strategic Business Plan.

The organization must begin to recognize security at that level in the organization where appropriate resources can be allocated to implement security effectively. The ISA begins at the strategic level, through planning and support from executive management. The first step of the ISA is to include security in the goals and objectives of the Strategic IT Plan. This will ensure that the integrated efforts of the many individuals responsible for security throughout the organization are moving toward a common objective that is realistic, reachable, and appropriately supported by the key business leaders.

GETTING STARTED

To evaluate how well an organization is positioned for developing an ISA and to gauge the level of emphasis that management is placing on controls and security in the processing environment, answer the following questions:

1. What type of processing environment exists in the organization (centralized, decentralized, hybrid)?
2. Is the processing environment network-centric? Are there LANs/WANs, remote access applications, Internet connections, business partner gateways (EDI)?
3. Who is responsible for the security of this environment (data security officer)?
4. Is there a regularly scheduled meeting/committee to address security issues?
5. What are the threats and risks in the organization's particular industry (e.g., aerospace → corporate espionage, banking → fraud)?

6. Have there been security incidences published that have occurred within the organization's particular industry? Were the losses quantified? (One will want to research this to provide supporting arguments for obtaining sufficient security resources.)
7. Have there been security incidences within the organization (i.e., viruses, system failure, lawsuits, desecration of Web site, disgruntled employees)?
8. Are any of the organization's sites located in areas of high probability for natural disasters (i.e., flood, earthquake, tornado, airport flight path)?
9. Do security policies exist (i.e., Internet, e-mail, confidentiality statement, new hire checklists, termination checklists)?
10. Do security standards and procedures exist and are they documented?
11. Does a Strategic Business Plan exist?
12. What are the business objectives listed in this plan? Does it include the use of IT to meet those business objectives?
13. Does a Strategic IT Plan exist? Are its objectives in direct support of the goals and objectives listed in the Strategic Business Plan?
14. Does either plan reference the reduction of risk as one of its objectives?
15. Does the Strategic IT Plan include the development of a secure processing environment as one of its goals and objectives?
16. Who developed or is responsible for the development of these documents?

Research the answers and use this research to begin the development process for the ISA. If unsure of the answers — or in answering them, come to the realization that security and control have not been a priority of key business leaders, and that the responsibility for security has not been clearly defined — the organization is most likely in need of an ISA. In researching these questions, one will begin to understand one's own level of knowledge related to the current controls in the processing environment as well as what controls alignment is necessary to reduce risk. An ISA is not something one can purchase. It is the process of developing an awareness of risk, an assessment of the current controls, and the alignment of controls to meet the security requirements of the organization. ISA development requires participation at all levels of the organization and only through this participation will an effective architecture begin to emerge.

Notes

1. Murray, W. H., Enterprise security architecture, *Handbook of Information Security Management*, Krause, M. and Tipton, H. F., Eds., Auerbach Publications, New York, 1998, 364.
2. Murray, W. H., Enterprise security architecture, *Handbook of Information Security Management*, Krause, M. and Tipton, H. F., Eds., Auerbach Publications, New York, 1998, 365.
3. Tipton, H. F., Enterprise security architecture, *Handbook of Information Security Management*, Krause, M. and Tipton, H. F., Eds., Auerbach Publications, New York, 1998, 5.

Chapter 2

Security Organization / Infrastructure

Within the business there must be an organization designated with the responsibility of information security management. This organization begins at the top with a high-level information security steering committee accountable at the highest level to the board of directors, president, or CEO to provide strategic direction and funding for the necessary components of the ISA (Information Security Architecture). This chapter discusses in detail the responsibilities of that steering committee and the subordinate security groups that implement information protection throughout the organization.

This chapter discusses the security organization as an entity of the main business. Previously, the main business, company, or corporation was referred to as the organization. This chapter refers to the main business as the enterprise so that the main business is not confused with the topic of this chapter, the security organization or infrastructure.

Learning Objectives

When finished reading this chapter, the reader should be able to:

- Understand the key players within the security structure of the enterprise.
- Understand the security roles of each individual in the security organization.
- Document resource ownership using the example matrix.
- Understand the challenges of developing a functioning and effective security organization.
- Understand the Strategic IT Plan and how the security architecture must be identified within it.
- Use the tools provided to initiate an ISA project.
- Define the following key terms:
 - Information or resource owner
 - Custodian
 - Internal audit
 - External audit

INFORMATION SECURITY ARCHITECTURE

- Component audit
- Compliance audit
- Security Coordinator or Liaison
- Security Team
- Executive Committee for Security

The Security Organization

The size and number of individuals participating in the security function will depend on several factors, including:

- Size of the enterprise
- Systems environment (distributed versus centralized)
- Number of components in the operating environment
- Organizational and management structure of the enterprise
- Number and locations of operational sites (i.e., national versus international)
- How the sites are interconnected
- Assessed risk
- IT Strategic Plan
- IT budget

The security organization, regardless of its size or naming conventions, should have the same logical structure and functionality for all enterprises. This logical structure and functionality is the subject of this chapter and can be scaled and tailored to meet the specifications of the enterprise. This chapter also discusses resource ownership and provides a project management approach for the development of the ISA.

One of the key challenges organizations have faced is the migration of the security function from a centralized, mainframe-based function to an effective governing body in the distributed systems environment. Establishing a strong, highly visible, and flexible security organization supported by executive management will provide the framework for increasing security awareness, minimizing information security risk, and providing the management structure for implementing and supporting security solutions.

In the past, the data security officer, whose chief responsibility was to administer user IDs, passwords, and access privileges, usually handled the security function in the centralized processing environment. The shift from terminal-based computing to PCs and the implementation of LANs, WANs, databases, and remote and Internet access created the requirement for significantly more security resources managed in a quite different manner from the centralized data security role.

One of the primary challenges that IS departments face is understanding the different security requirements for all of the technology implementations within the enterprise. The most common problem is that security

responsibilities for new technology implementations are usually handed to those individuals performing application or operating system access control because “access control” is clearly a security function that was the main focus when security awareness came about in industry. Those responsible for access control may not have a technology background in areas such as remote access, e-mail, Internet, and LAN/WAN operating system vulnerabilities.

Placing the security responsibility on an individual who is not trained in the technology being implemented can result in a false sense of security. The most common example of this has been with firewall implementations. Firewalls became popular when enterprises began using the Internet for e-mail and electronic commerce. Hiring an individual with firewall experience was difficult and costly because firewalls were relatively new to the business environment and there was not an abundance of skilled firewall technicians. Five years ago it was rare that an individual was hired just to implement a firewall. What resulted was that existing IS personnel, and most likely the data security officer, were asked to make sure the enterprise Internet connection did not present a problem similar to those being publicized daily in the media. With little or no experience in firewall implementations, IS personnel were selecting, implementing, and maintaining firewall solutions — albeit not effectively.

The second challenge for security is obtaining adequately budgeted resources. This includes formalized training, management and assessment tools, and adequate time to perform security responsibilities. Security personnel have the right to be appropriately trained to perform their security responsibilities. Too many times, however, it is security training that is cut from the training budget because management feels that security is a skill that can be picked up or learned through hands-on experience. Many security individuals have learned much of their skills from self-initiated hands-on “playing” rather than formalized training. The cost of an incident, because the security owner did not fully understand the scope of his or her responsibilities, can far exceed the cost of several training courses.

Management and assessment tools are necessary to assist security personnel in performing their duties more efficiently and effectively. Examples of these tools can be readily found on the Carnegie Mellon University Web site at www.cert.org. A search of “tools” on the CERT’s search engine yields tools that:

- Report system events
- Report network events
- Report user-related events
- Verify data, file, and software integrity
- Examine systems in detail
- Check for Trojan horses

INFORMATION SECURITY ARCHITECTURE

Many of these tools are available as free downloads. Without these tools, administrators must know exactly what they are looking for and must perform manual queries that take significantly more time. The more time it takes, the less likely that all of the security checks and procedures will be performed. Tools enable the administrator to quickly target an area of vulnerability and then manually drill down on the potential issue. Chapter 4 lists in detail the specific tools, their functionalities, and where they can be found on the Internet.

IS personnel, especially during technology implementations, tend to be overutilized. Security is often added as an additional duty to someone who already has a full-time job maintaining the existing environment, has been handed the additional responsibility of a new technology implementation, and must also find the time to ensure that security procedures are defined, implemented, and maintained. In all probability, it is the security responsibility as an additional duty function that falls to last priority simply because current systems must be maintained, new implementations are highly visible and must succeed, and there is just no time left over to perform security procedures. Only until the past several years have security incidences relating to the Internet served to increase awareness among senior management, and this has resulted in an increased demand for appropriate security resources.

The ISA requires the necessary resources and organizational structure to continue with the security plan. These resources include individuals responsible for developing, approving, and implementing security policies, procedures, and standards, as well as the vehicle to conduct periodic sessions to address issues as they arise. Defining the security organization and infrastructure is the first step of ISA development because it is necessary to assign ownership for the ISA project as well as the ongoing execution of security responsibilities. This is done by identifying those individuals within the enterprise who are currently responsible for security or to some degree execute security procedures whether or not the procedures have been formally identified and documented. It is then necessary to restructure and redefine their security roles and expand their security responsibilities within a framework that is understood and supported.

Who are the key players of the security organization? The Chief Information Officer (CIO), the Chief Financial Officer (CFO), the Security Officer, security coordinators or liaisons, application coordinators, Human Resources, Legal Counsel, help desk, department management, and all system and information users. All of these individuals play some role in the development, design, and implementation of security and will more than likely have membership in one of three groups, the Executive Committee for Security, the Security Team, or the User's Group.

The Executive Committee for Security

The Executive Committee for Security is comprised of director-level management who is the approval authority for all security plans relating to the protection of enterprise systems and electronic information assets. This Committee is responsible for ensuring that the objective of a secure operating environment, through the establishment of an ISA, is clearly defined in the enterprise strategic plans. This Committee or members of this Committee are the project sponsors for the ISA. Without their support, adequate resources will not be available to develop and implement the ISA.

Smaller organizations may not feel that they are large enough to establish a separate committee for security. The roles and responsibilities of an Executive Committee for Security can be incorporated into an existing committee's charter to ensure that security and confidentiality issues and initiatives are addressed at the highest level of the enterprise. Whether an existing committee assumes responsibility for security or a separate committee is formed, the Committee will be responsible for reviewing the Security Policy and for ensuring that all implementation plans, procedures, and standards are consistent with the overall risk management and protection expectations of senior management.

Where these responsibilities reside will be a function of the size of the enterprise. In some enterprises, they reside with the Board of Directors. This is typical with smaller businesses that do not have the human resources to support separate committees or do not have a deep vertical infrastructure. The name of the Committee is not extremely important as long as the approval authority for security exists and is operational. The functions of the Executive Committee for Security have resided at the Executive Counsel, the Information Technology Counsel, and the Board of Directors. Members usually include the CEO, the CFO, the COO, the CIO, the Security Officer, department or business unit directors, advisors to executive management, and/or members of the Board of Directors, as shown in Exhibit 2-1.

The Chief Information Officer

The mission of the Chief Information Officer (CIO) is to provide technology vision and leadership for developing and implementing IT initiatives that create and maintain leadership for the enterprise in a constantly changing and intensely competitive marketplace. The CIO is responsible for:

- IT policy and aligning IT strategy with business strategies
- Business technology planning process, including the sponsorship of collaborative planning processes
- New and existing applications development for enterprise initiatives and overall coordination for business unit or divisional initiatives

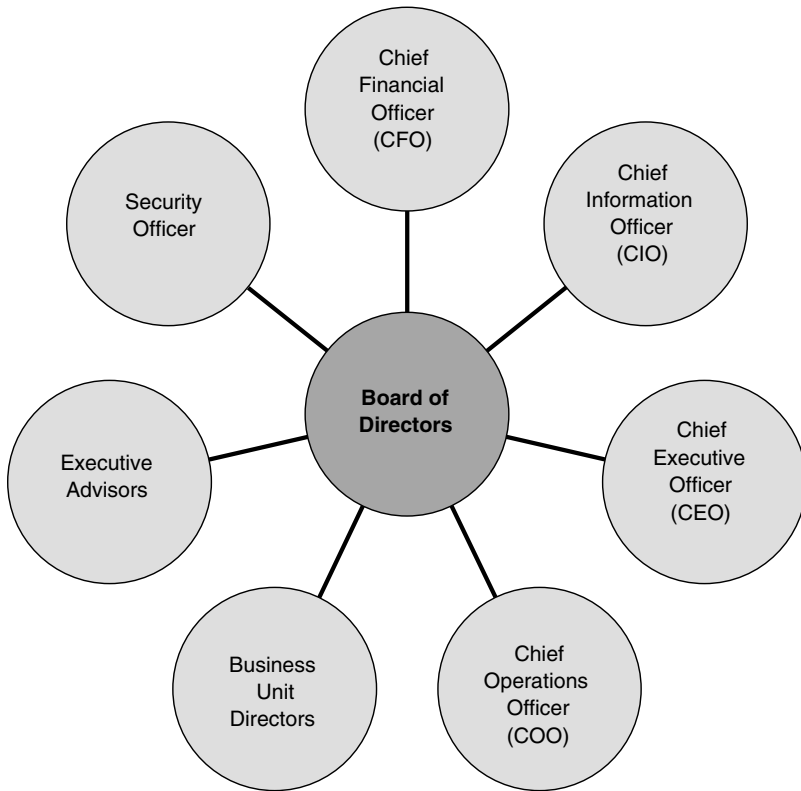


Exhibit 2-1. Executive Committee for Security

- IT infrastructure and architecture (e.g., computers and networks) operations and investment decisions
- Sourcing and purchase decisions, which include make versus buy decisions relative to outsourcing, versus in-house provisioning of IT services and skills
- Establishing partnerships, including strategic relationships with key IT suppliers and consultants
- Technology transfer by providing enabling technologies that make it easier for customers and suppliers to do business with the enterprise as well as increase revenue and profitability
- Customer satisfaction with internal and external clients to ensure continuous customer satisfaction
- Implementation of security initiatives related to all IT components to protect the infrastructure and reduce risk to a manageable and acceptable level
- Providing training for all IT users to ensure productive use of existing and new systems¹

The ISA is an infrastructure issue aimed at reducing risk to the business so that the strategic business objectives can be realized. The CIO is the most likely proponent for the ISA project because many of the highly specialized security functions for components such as LANs, databases, and firewalls logically reside within the IS organization.

The role of the CIO in information security is to communicate to executive management the business risks of implementing new and distributed technology and the necessity for developing the appropriate security infrastructure to carry out the ISA.

The Chief Financial Officer

The CFO is the enterprise's principal accounting officer and typically has responsibility for all planning and control functions within the enterprise. The CFO must ensure the timely and accurate execution of all enterprise accounting functions. This includes understanding and consolidating financial, internal and external (SEC and shareholder) reporting, inventory credit, accounts payable, fixed assets, and payroll activities. The CFO oversees the development of all appropriate financial information systems that support these functions. It is important that the CFO and his or her staff maintain leading-edge technical knowledge. Specific responsibilities include:

- Determining and maintaining the adequacy of internal controls to ensure that enterprise assets are safeguarded and liabilities are appropriately minimized
- Ensuring the adequacy of accounting systems and procedures to enable the accurate reporting of the company's financial position and operating results, and the proper recording of corporate transactions
- Directing the preparation of internal monthly, quarterly, and annual financial and operating results
- Ensuring the accurate and timely preparation of external SEC and shareholder reports, as well as those required by other institutions
- Overseeing the development of financial information systems enterprisewide to promote the timely and accurate assimilation, consolidation, and reporting of financial results and position
- Supporting the ongoing IS projects and improving the strategic capabilities of the Controller's function to balance its existing tactical strength²

The CFO is ultimately responsible for all strategic planning, control, and risk assessment related to the enterprise. The risk responsibilities of the CFO originate with the financial health of the organization. With information technology tied directly to the accomplishment of the enterprise business objectives, risks and exposures related to information technology can

INFORMATION SECURITY ARCHITECTURE

unequivocally affect the bottom line of an enterprise. Managing IT risk becomes a major responsibility of the CFO. It is the CFO and CIO who share the responsibility for information and technology risk and controls, and they must work together as joint sponsors of the ISA project and ongoing security implementations.

The Security Officer

The Security Officer has overall responsibility for information security matters, is a member of both the Executive Committee for Security and the Security Team, and acts as liaison between the two. The Security Officer's responsibilities are to:

- Communicate with executive management on the risks and controls related to the business and operational systems environment
- Ensure that appropriate user access and authentication controls are in place
- Ensure that the documented security policies, standards, and procedures are reviewed, updated, and maintained periodically by appropriate individuals
- Evaluate security exposures, misuse, or noncompliance situations, and ensure implementation of security controls to address those incidences
- Ensure that all business unit/department Security Coordinators understand and execute their security responsibilities in accordance with related policies, standards, and procedures
- Organize and conduct periodic Security Team meetings
- Research security Web sites, CERT advisories, publications, vendor correspondence on application patches, updates, and version releases, and the media for recent exposures and their fixes in operating systems and networks
- Develop and implement the Security Awareness Program with assistance from Security Team members
- Develop and implement the Review and Compliance Program with assistance from Security Team members

The Security Officer is responsible for leading the efforts of the Security Team. The role of the Security Officer within the ISA and the distributed processing environment should not be confused with the role of the Data Security Officer from the mainframe environment. The Security Officer is the coordinator of all information security activities. There are many other individuals who participate in the actual development and implementation of the security policies, standards, and procedures. For example, the Security Officer is not solely responsible for writing the Security Policy; that is the role of the members of the Security Team. The Security Officer is responsible for making sure that the Policy gets written, and is appropriately distributed and

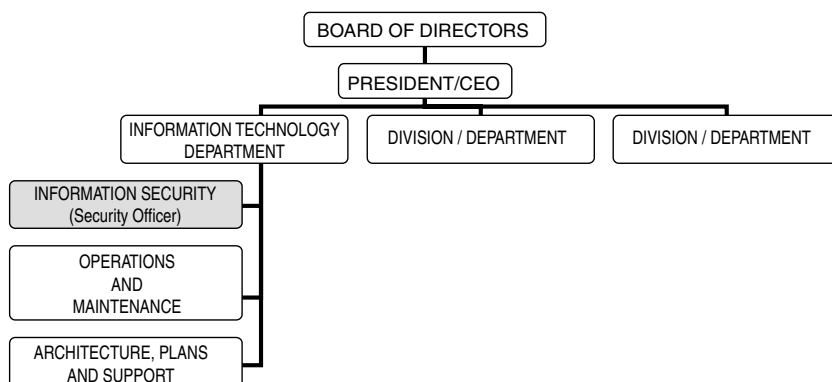


Exhibit 2-2. Security Officer Placement (Typical)

enforced. One of the key reasons why security fails is lack of employee involvement and ownership in the security program. Development of policies, procedures, and standards must be through the participation of those individuals responsible for implementing and following them. The main duty of the Security Officer is not to perform all security-related functions, but rather to ensure that security efforts are coordinated; policies, procedures, and standards are developed and followed; and the security program is effectively implemented and updated according to changes in the processing and business environment.

The Security Officer should report to executive-level management. Usually, this is a member of the Executive Committee for Security and, more than likely, the CFO or the CIO. Typical placement of the Security Officer within the organization is shown in Exhibit 2-2.

When the ISA in the enterprise has become mature through several cycles of assessment, mitigation, audit, and effective compliance, the Security Officer role should be taken out of the IS venue and report directly to the president, CEO, or Board of Directors, as shown in Exhibit 2-3.

The higher in the organization a Security Officer resides, the more emphasis, support, and visibility is placed on the role of security in the enterprise. With the Security Officer on the same level as the CIO and no longer a direct report to the CIO, the CIO is no longer auditing his own processes, which can be viewed as a conflict of interest.

The Security Team

The Security Team is the primary vehicle for communicating to management the risk control strategies that are being considered for implementation across sites and reporting management's concerns about these protection measures. It is recommended that the Security Team consists of the

INFORMATION SECURITY ARCHITECTURE

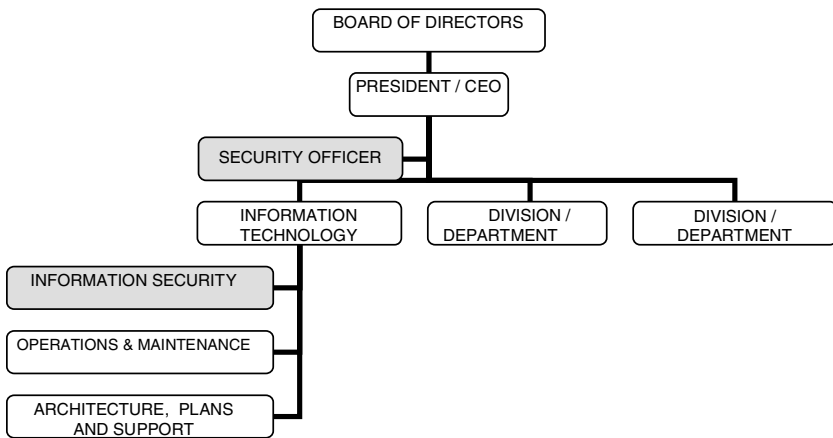


Exhibit 2-3. Security Officer Placement (Mature Security Life Cycle)

Security Officer, security coordinators or liaisons from each department or business unit, network and applications administrators, and representatives from Legal Council, Human Resources, and the Information Systems department, as shown in Exhibit 2-4. Membership on the Security Team, if not already established, should be identified to assist with the development of the ISA project.

Specific functions of the team, together with operations management, are to:

- Represent particular security and business continuation issues and concerns within each enterprise location
- Identify risks within each member's area of concentration and ensure that appropriate controls are implemented to address these risks
- Develop, review, and recommend all security policies, standards, and procedures that will be implemented across sites
- Develop and implement an Information Security Awareness Program for all information technology administrators, development personnel, users, and their management, and administer the implementation of this program within their area
- Create and maintain the security architecture as well as champion the implementation process

Initially, the Security Team will perform the majority of work on the development of policies, standards, and procedures for the ISA, and the Executive Committee for Security will approve all work products of the Security Team. Once the ISA has been developed, the members of the Security Team may change and the focus of the Team will shift to security implementations; a concentration on current issues; review and modification of existing policies, standards, and procedures related to changes in the

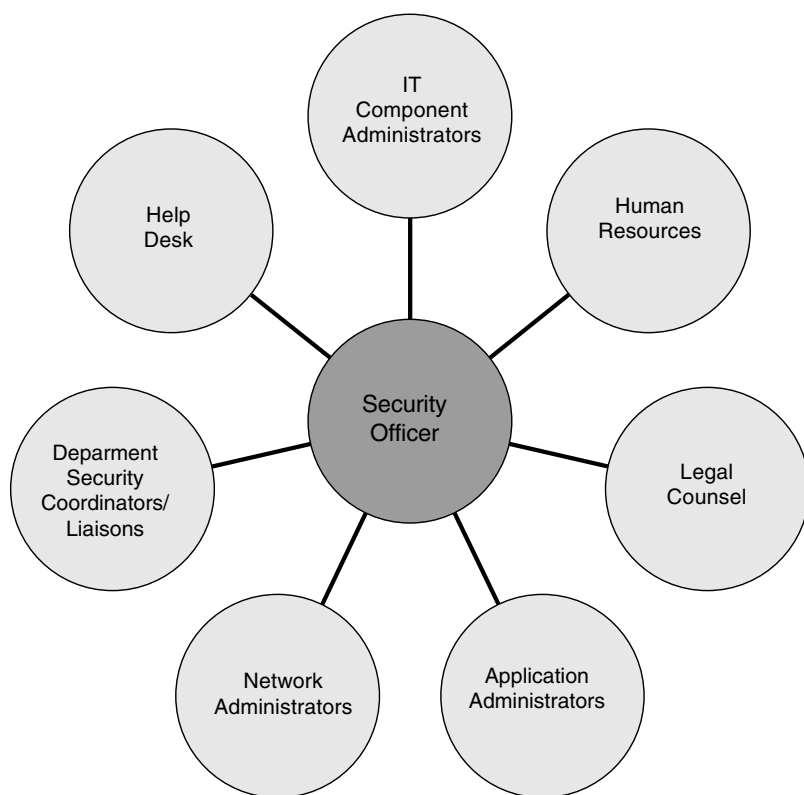


Exhibit 2-4. The Security Team

technology environment; and periodic risk assessments to identify new vulnerabilities. For example, Human Resources and Legal Counsel will play a lesser role in meetings once policies and procedures have been written, reviewed, validated, and implemented. Security owners, and network and application administrators will be concerned with baseline security assessments of their components and improvements to the current control environment. The Team then may be more applicably renamed to the Security Council or Security Advisory Committee to provide advice and counsel on current issues and decisions.

Security Coordinators or Liaisons

Security coordinators should be assigned within each location, department, or business unit to establish the security policies, standards, and procedures within the sub-unit and to coordinate with the department business managers on security-related issues. The coordinator's primary responsibility is to ensure that appropriate user access within the scope of their business function is maintained. Additional responsibilities include:

INFORMATION SECURITY ARCHITECTURE

- Ensuring that application access forms are initiated for existing and new users within the respective departmental area
- Ensuring that access is modified or deleted when employees and non-employees (i.e., consultants, contractors, business partners) operating within their business function or site are transferred or terminated
- Conducting user security awareness within their departmental function
- Ensuring that the enterprise Confidentiality Agreement and exit interview forms are signed by all users operating within their department or area of responsibility
- Actively participating as a member of the Security Team
- Coordinating with the Security Officer on all security-related matters

Depending on the size of the enterprise and the number of security coordinators or liaisons, these individuals may choose to meet as a separate advisory group to discuss best practices for establishing and maintaining security at the business unit level.

Departmental Management

Departmental management refers to enterprise managers who are responsible for functional business areas. Reference to departmental management within this book generally means the head or a designated person who has the responsibility and authority to act on behalf of senior management. This person is also considered the owner of the information. For example, the Chief Accountant or Head of the Accounting Department is responsible for the accuracy of and access to all accounting information and systems. This includes general ledger, accounts payable, accounts receivable, fixed assets, etc. When something is in error with the financial reporting from this department, it is the Chief Accountant or Head of the Accounting Department who is ultimately responsible. It is the Chief Accountant who owns (or is responsible for) the accounting application and information. In this sense, it is the Chief Accountant who should have the final say regarding the levels of access for each individual accessing modules of the accounting package.

Departmental management is responsible for establishing the overall security strategy for department information. This includes determining the security classification of information owned by the department. Classifications will indicate the level of sensitivity and availability required for the information. In addition, department management is responsible for authorizing the level of access to information within each respective department function.

Network and Application Administrators

Network and application administrators are technically responsible for the operation of the network or application. These administrators are responsible for assisting the departmental manager in implementing and managing information technology policies, procedures, standards, and departmental guidelines for a particular component of the operating environment. They are trained to maintain the system and must coordinate with both departmental management and security coordinators (liaisons) to implement appropriate access controls for this component. The difference between the security coordinator (liaison) and the network administrator is that the security coordinator works within the business unit and is aware of the appropriate access policies for each employee within that department or business unit. The network and application administrators actually implement the access control policies for each individual but may have no knowledge if the access is appropriate. The application administrators and security coordinators work together as a check and balance for access control.

Another responsibility of the network and application administrators is to establish the baseline control standards upon completion of a risk assessment and the identification of vulnerabilities. This is described in further detail in Chapter 4.

Human Resources

The Human Resources Department is responsible for managing and coordinating hiring, termination, and disciplinary practices within the enterprise. Human Resources and departmental management are responsible for providing timely information to the enterprise LAN managers and application administrators about employee termination or transfers so that appropriate steps can be taken to revoke or change access to systems and information. Human Resources can also ensure that new hires will be given the opportunity to read the Security Policy and Confidentiality Agreement and sign an acknowledgment form. In addition, Human Resources can ensure that an exit interview is conducted and, if necessary, reaffirm the obligations of confidentiality by having the employee read once again and sign the Security Policy and Confidentiality Agreement upon termination of employment. The Human Resources representative is actively involved in the establishment of policies and may participate less often in security meetings once those procedures have been established.

Legal Counsel

A legal representative should be a part of the Security Team or the Executive Committee for Security and have the responsibility for reviewing all security policies and procedures for enforceability. Issues related to

INFORMATION SECURITY ARCHITECTURE

breach of confidentiality, misuse of information, or destruction of information, files, or programs are often cause for termination or the subject of legal liability. Common security procedures such as monitoring e-mail (an enterprise-owned resource) must be implemented according to the law. The law indicates that monitoring procedures will be disclosed to the users of the application or resource. Lawsuits have been won against the enterprise in cases where the enterprise failed to inform the user that monitoring was taking place. Enterprises have also lost lawsuits against hackers in cases where the enterprise failed to appropriately warn the hacker of the enterprise's security policy or failed to prove that they had made an effort to protect their information and processing resources from intrusion.

The use of the Internet and electronic commerce has initiated new legal issues that cannot be answered by existing laws. Laws related to electronic commerce, electronic correspondence, and the use of enterprise resources have been the subject of review and modification by the legal system. It is necessary for the enterprise's legal counsel as well as the security organization to stay abreast of these modifications to ensure that enterprise policies do not contradict the law. Legal counsel must be aware of the legal issues related to wiretapping, encryption, intellectual property, trade secrets, computer and credit card fraud, patents, copyrights, and trademarks. For certain industries such as healthcare and banking, information protection laws have also been implemented, as indicated below. The following laws and regulations should be reviewed and understood when developing security policies and procedures:

- Electronic Communications Privacy Act of 1986 (ECPA)
- U.S. Wiretap Law (as amended by the ECPA) 18 U.S.C.A. § 2510 et al.
- Computer Fraud and Abuse Act of 1986, 18 U.S.C.A § 1030
- Federal Trade Secret Law — Espionage Act of 1996, 18 U.S.C.A. § 1831 et al.
- Credit Card Fraud — 18 U.S.C.A. § 1029
- U.S. Telecommunications Act, Title V: § 223(a)(1)(b) and §223 (d)(1)
- The Communications Decency Act
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley
- FDA 21 CFR Part 11
- California SB 1386
- Homeland Security Act of 2002 (HSA)
- Patent, copyright, and trademark laws
- State laws regarding wiretap, espionage, and computer fraud

Legal counsel should also be tasked to assist in developing user awareness training related to these issues and the applicable federal, state, and local laws and regulations.

Help Desk

The Help Desk centralizes customer service for support of predominately hardware, software, and technology assistance. Services of the Help Desk related to hardware and software include asset inventory, management, and retirement; acquisition; maintenance and installation; moves, adds, and changes; planning and design; preventative maintenance; product evaluation; software support, including dispatched, on-site, and by phone; system integration; technology refreshments; and troubleshooting. Help Desk software provides the means to log all calls and provide follow-up to unresolved or ongoing issues. It also offers a historical view of trouble areas within an enterprise. The Help Desk can be the keeper of enterprise policies, standards, and procedures — often online — so that advice and guidance can be quickly retrieved and given in compliance with policy.

Related to security the Help Desk is a good first-level contact who can direct the security issue to the appropriate individual and provide appropriate follow-up and documentation. In addition, when a penetration or attack is in progress, the Help Desk might receive a concentration of calls on a particular topic and can minimize the damage by quickly identifying and tracking the problem.

Audit

There are four levels of audit functions related to the ISA: (1) the internal audit function, including electronic data processing (EDP) auditing; (2) the external audit function required by the SEC, NYSE, NASDAQ, and AMEX and performed by public accounting and auditing firms; (3) component audits performed by the system administrators and security liaisons; and (4) compliance audits performed by the Security Officer and Security Team. Despite the fact that the internal and external audit functions focus on the requirements of the SEC in financial reporting, an integrated approach to implementing all four audit functions is necessary to ensure adequate internal controls within the enterprise and provide increased security effectiveness.

Internal Audit. Many companies will have an Internal Audit Department or function whose primary responsibility it is to assess risk, measure compliance to policy, validate financial reporting, and provide corporate governance. The group or individuals performing the audit function must:³

- Understand the organization's business, the accounting process, and internal control concepts.
- Assess risk at the account and potential error levels.
- Plan the audit approach and test of controls.
- Test controls and ensure that adequate internal controls are in place.
- Review the corporate code of conduct and monitor compliance with it.

INFORMATION SECURITY ARCHITECTURE

- Ensure integrity and objectivity of financial statements.
- Review financial statements and recommend their approval to the board.
- Oversee the company quarterly reporting process.
- Consider selection, implementation, and impact of significant accounting policies.
- Review management judgment of accounting methods and estimates.
- Understand financial and operational issues.
- Participate in activities designed to prevent and detect fraud.
- Remain independent of management.
- Review legal company obligations and pending litigation.
- Review company insurance coverage.
- Review compliance reports to regulatory agencies.
- Review company budgets and executive expenses.
- Participate in the selection of external auditors to enhance their independence.
- Review external auditors' findings and communicate with external auditors on financial issues.
- Monitor management responses to external auditors.

The audit function is designed to protect the organization's financial and operational resources. The audit function must also include IS (EDP) auditing. The main objective of the IS auditor is to provide expertise in conducting audits of data processing systems to determine and ensure compliance with prescribed policies and procedures. The IS auditor will:

- Analyze a system or component to formulate the best approach for performing the audit.
- Prepare audit workplans for each system or component.
- Review the system's processes and documentation to determine compliance with stated data processing standards.
- Review the system's input and output to verify the correctness of the transaction processing and reports.
- Ensure that systems produce the desired information.
- Evaluate and review proposed applications to provide input into the design of new systems regarding internal controls and adaptability.
- Periodically review data processing facilities to ascertain organizational and operational effectiveness.
- Provide audit support to other audit staff.
- Coordinate the use of IS audit procedures for operational and financial audits.
- Examine computer systems documentation and output to ensure the presence of adequate controls.
- Develop audit reports and recommendations to IS and business management that identify irregularities or deviations from established policies and procedures.

In situations where a company does not have IS auditors, strong consideration should be made for IS audit outsourcing. Some companies feel that when substantive testing is performed related to the financial audit, that IS auditing is not necessary. Much of the information and reports used to perform substantive testing for financial audits are system generated, placing a significant reliance on the processing environment. Open systems and distributed processing environments increase the number of access points into the processing environment, producing additional security risks. Whether a qualified IS auditor exists within the organization or the IS audit function is outsourced, risk assessments of technology should be performed to understand the realistic risk to the enterprise and must be communicated to management for appropriate decision making on risk reduction.

External Audit. The external auditor is the financial statement auditor required by public companies to attest to management's assessment of the effectiveness of an entity's internal controls using standards that the Public Company Accounting Oversight Board issues or adopts.

Auditors perform procedures to obtain sufficient evidence to express an opinion as to whether an entity has maintained, in all material respects, effective internal control over financial reporting as of a point in time based on "control criteria." This control criteria includes:

- The control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

These control criteria are evaluated in three categories: (1) effectiveness and efficiency of operations, (2) compliance with laws and regulations, and (3) reliability of financial reporting.

In response to the highly publicized business failures, allegations of corporate improprieties, and financial statement restatements, Congress enacted the Sarbanes-Oxley Act of 2002, which has modified the rules of external audits. It is necessary for management to understand these changes. The American Institute of Certified Public Accountants (AICPA) Web site (<http://www.aicpa.org>) provides information on internal control and integrated framework requirements as well as AICPA audit and attest standards published as Statements on Auditing Standards (SAS).

Enterprises that do not have an internal or external audit function outsource their operations to a third-party processor, and do not have the expertise to ensure the control environment of their outsourced operations should consider obtaining consulting services to validate the third-party processor's control objectives.

Component Audits. Component audits are performed by the system administrators and security liaisons for each technology implementation. Applications, operating systems, databases, networks, and hardware come with standard configurations that rarely emphasize secure operation right out of the box. Component audits will be discussed in more depth in Chapter 4, “Security Baselines and Risk Assessments.”

A security baseline is the starting point of understanding the vulnerabilities and risks of a system component’s configuration. As the security features of the component are studied and understood, the features to provide more secure operation can be enabled. This should be done during implementation and as user access is added to the system. Additionally, standard operating procedures (SOPs) must be documented for each component to ensure the most secure operating configuration. System components usually come with basic documentation on secure mode operation; however, enterprise-specific procedures should be further defined. The security baseline or component audit provides the knowledge to develop the enterprise-specific SOP.

Compliance Audits. Once it is clearly understood, through documentation and component audits, how a component is to be configured and utilized, compliance audits provide the testing procedures to ensure that the SOP is being followed. Compliance audits for the ISA are performed by the Security Officer and Security Team. In an integrated approach, audits performed by EDP auditors from both internal and external audits can be used or relied upon for the compliance function. The main difference between baseline (component audits) and compliance audits is that the baseline is a mechanism for discovery and development of secure operation. In the compliance audit, secure operation is known and documented and is merely being tested to ensure conformity. Compliance audits must be performed on a periodic basis.

System Users

System users include any employee, contractor, vendor, consultant, or business partner of the enterprise who uses information systems resources to perform his or her job function. Their security responsibilities include:

- Maintaining the confidentiality of passwords
- Ensuring security of information they are privileged to as a part of their job
- Using enterprise resources for management-approved purposes only
- Adherence to all information security policies, standards, and procedures
- Reporting any issues or security incidences to management

To hold users accountable for these responsibilities, they must first be made aware through a user awareness program and through published, disseminated, and enforced policies, standards, and procedures. Assuming that an employee will read the policies, standards, and procedures is not enough. Obtaining a signature from the employee that he has read and understands the policies and his responsibilities provides a mechanism to show due process. Educating the user on the threat, risk, and consequence of not ensuring his responsibilities is critical to effective user participation in security.

Centralized versus Decentralized Security Administration

What was once a centralized function is now best handled by a hybrid between centralized and decentralized security administration. It is necessary to establish the Executive Committee for Security and the Security Team as a centralized function for appropriate security decision making and policy development. Centralization of the Security Team provides the vehicle for communicating common issues and solving problems through internal resourcing. It also provides a central point of accountability, separation of duties, and the benefit of economies of scale through standardized solutions.

The Security Team described in this chapter meets as a centralized function; however, individuals throughout the organization staff it. Those individuals, with the exception of the Security Officer, have primary responsibilities other than security. As a member of the Security Team, they have a dotted-line report to the Security Officer. In this sense, the Security Team is not truly centralized. It is becoming more common that organizations with significant risk have adopted a truly centralized security organization that is staffed with full-time positions dedicated to the security of the enterprise. These individuals should have a direct-line report to the Security Officer. With a dedicated security staff, the Security Team and its members as previously described will continue to operate with the same functionality to promote security throughout the enterprise and will continue their specific decentralized security responsibilities. Some security administration and execution of responsibilities should continue to be distributed to the business units through the security coordinators (liaisons), application owners, and department management. The one exception to this is that new technology initiatives should remain centralized at the corporate level so that these new projects receive the necessary resources, coordination, and guidance. Once training and implementation are complete, security administration for the new initiative can be moved to the primary business unit or beneficiary of the system.

The dedicated security organization will supplement the Security Team as the consolidator of all ISA documentation, with research and development

INFORMATION SECURITY ARCHITECTURE

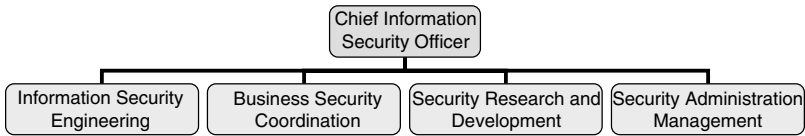


Exhibit 2-5. Proposed Information Security Risk Organization

of security products, security product implementations, training, risk assessment, and coordination of activities between business units.

Back in February 1996, the Gartner Group wrote a strategic planning assumption paper entitled “On the Organizational Placement of Information Security.” The Gartner Group ascertained that the majority of individuals performing security functions were assigned to the IS department because “although these individuals (reported) in a matrixed fashion to the quasi-independent security team, they were in fact full-time operational personnel in the technical support organization within the IS group.”⁴ The issue that arises with full-time operational personnel in the IS group performing security functions as an additional responsibility is that security is secondary to their operational role and they are tasked with policing their peers within the IS department. The full-time staff within a separate and dedicated security organization provides true separation of duties and eliminates the issue of policing one’s peers within the same department.

The Gartner Group predicted a realignment of the corporate information security department as an independent line organization. The Gartner Group indicated that this was already occurring in several large banks, stock brokerages, insurance firms, hospitals, and government agencies because of the significant risks these industries have incurred. These organizations “were experimenting with (1) placing the information security function within corporate legal or other line organizations, or (2) appointing a senior executive — the “chief information security officer” — who reports to the board of directors and is responsible for coordinating all information security issues with audit, legal and line management areas.”

In an Information Security Strategies Research Note entitled “The Metamorphosis of the Information Security Organization,” the Gartner Group defines the dedicated security organization as having four dedicated security groups that perform security engineering, business unit coordination, research and development, and security administration management (see Exhibit 2-5).⁵

The primary responsibilities of each group include:

1. *Information security engineering.* Create and maintain the ISA; perform security baseline assessments, user security awareness and training, and security solution implementations.

2. *Business security coordination.* Coordinate with business units through security liaisons to establish business unit policies, standards, and procedures that are in line with corporate guidance and policies.
3. *Security research and development.* Research emerging security technology such as firewall products, single sign-on, encryption, password generation, and secure internetworking.
4. *Security administration management.* Act as the approval authority for security administration decisions and the work of the Security Team to ensure the most cost-effective and efficient security administration processes.

The functions of each of these sub-groups parallel those of the Security Team and the Executive Committee for Security. Many high-risk industries, such as defense, will have dedicated security organizations with staff specializing in each of these areas. In an industry such as healthcare, agencies such as the JCAHO (Joint Commission for Accreditation of Healthcare Organizations) govern the industry with regulations and policy related to patient confidentiality. Most healthcare institutions have created full-time positions for JCAHO Information Management Planning to handle current regulation and policy considerations for confidentiality.

Other enterprises either cannot dedicate resources to establish a full-time security organization due to resource constraints, will not do so due to their lack of understanding of the present risk, or have no need to dedicate resources due to limited technology implementations, limited risk, or size of the enterprise. In these instances, the Executive Committee for Security and the Security Team must continue to operate with available resources.

The Security Team should meet weekly while developing the ISA. Once the architecture has been defined, the Security Officer will determine how often the Team must meet. The lack of a dedicated security organization will impact meeting requirements as well as decisions, timing, and resources related to security solution implementations.

Information and Resource Ownership

Ownership of system components is often difficult to define because several individuals are responsible for different functions of a system. This confusion makes it doubly necessary to define and document these responsibilities so that those sharing ownership do not make inaccurate assumptions about what the other is doing. There are three levels of security responsibility:

1. Owner
2. Coordinator (liaison)
3. Custodian

INFORMATION SECURITY ARCHITECTURE

The example used previously was that of the Chief Accountant who owns (or is responsible for) the accounting application and information and has final say regarding the levels of access for each individual using modules of the accounting package to perform his or her duties.

The application administrator must also establish security ownership for the accounting package. The Chief Accountant understands the duties and functions of his staff. He also understands the risks and necessity for separation of duties in certain accounting transactions. The application administrator understands the application controls, risks of the operating system, and limitations of the system. These two individuals share ownership of the application and information, and must work together to ensure that weaknesses do not arise due to a lack of communication between them or the lack of definition regarding their specific responsibilities. This example succinctly demonstrates why security must be an integrated function and how it commonly breaks down because of the lack of communication, definition, and documentation of ownership responsibility.

To eliminate confusion, we define the *information (resource) owner* as the individual responsible for logically ensuring that the asset is properly safeguarded from unauthorized access, modification, disclosure, or destruction. In our example, this would be the Chief Accountant. In the case of information, the owner is the individual who created it. The application administrator who is physically responsible for implementing safeguards such as access control lists (ACLs) will be referred to as the *custodian* of the accounting information. The custodian of the information can be designated by the owner of the information. For specific components such as applications, the custodian is appointed by virtue of his position as the application administrator.

Confusion regarding ownership may arise because of the delegation of duties. A Chief Accountant might designate one of his managers to review and approve access. Does this alleviate the Chief Accountant from his responsibility as the application owner? No, it does not because it is the Chief Accountant who will be accountable to the CEO if something goes wrong with the accounting application due to the inappropriate administration of access. Let us continue on with this example. A disgruntled employee who has left the enterprise is inadvertently left on the system for several weeks. The former employee accesses the system and causes irreparable damage to critical system files. Is the Chief Accountant off the hook because he delegated the duty? Again, the answer is no. Initially, management will be interested in finding out why and how the incident occurred. Blame must always fall somewhere. Ultimately, the incident will have a negative impact on the individual who has overall responsibility for the business unit, and that is the Chief Accountant. In this case, the individual who has been delegated the responsibility of defining access is the *security coordinator (liaison)*.

A slightly different example is the component owner. Windows NT, 2000, XP Administrators are responsible for setting up user IDs and security defaults within the operating system. By nature of this position, the Windows operating system administrator is the owner of the Windows operating system and Windows security. This administrator, however, should not be held responsible for understanding each individual's level of access required to the information on the file server within each department. The Windows Administrator will work with a security liaison, or application owner within a sub-unit or department, to set up appropriate access. In doing so, the Windows Administrator becomes the custodian of the application data. This integrated security administration should be documented by defining each of the security owner, liaison, and custodial responsibilities and their interaction with each other related to an application, sub-unit or department, or network. It is recommended that an appendix to the Security Policy be used to document these positions, responsibilities, and names of the individuals within those positions.

The template in Exhibit 2-6 can be used to begin to identify all the components in the operating environment. This should include applications, platform operating systems, databases, and network operating systems. This form can be modified to meet the enterprise's individual needs. It is a tool to begin the identification process and, in so doing, user awareness is initiated through validation and acceptance of the security roles. For enterprises that have several administrators for the same platform, such as UNIX or Windows operating systems, each of these components should be listed and identified with the specific business unit or application that it supports. The "Level of Sensitivity" column is to identify those applications that require special consideration, whether they contain classified information or are critical to business operations and should be considered in disaster recovery planning/business continuity planning (DRP/BCP). The "Reference Documents" column indicates the documented procedures related to the protection of that specific component.

You may find many of those individuals identified as owners or liaisons who are hesitant to take on the responsibility or to have their name documented in the appendix. This is because they do not perceive any personal benefit for them to do so. For them it is an additional responsibility without additional compensation, positive recognition, or appropriate time to perform the responsibility. They often feel that being documented as the responsible individual is only to hold them accountable when something goes wrong. Additionally, some owners and liaisons feel that it is ultimately the custodian who is responsible because it is the custodian who physically sets the access rules.

How can you get the owners, liaisons, and coordinators interested in becoming effectively involved in these responsibilities? By having them be

Exhibit 2-6. Information/Resource Ownership

Resource/ Application	Product/ Business Unit	Resource Owner	Security Liaison	Security Custodian	Level of Sensitivity*	Reference Documents
Business Systems						
EDI						
Facilities Management						
Time/Attendance						
Human Resources						
Accounts Payable						
General Ledger						
Fixed Assets						
Payroll						
Budgeting						
Purchasing / Materials Mgt.						
Network Support System						
Routers						
Remote Access						
Windows XP	Accounting					
Windows 2000	Manufacturing					
UNIX	Research & Development					
* Sensitivity						
1 — high						
2 — medium						
3 — low						

an integral part the ISA project. This is the starting point of user awareness and training for the security owners, liaisons, and custodians. The identification of these security owners, security liaisons, and custodians should be documented by position. This can best be accomplished if security responsibilities are written into job plans so that these individuals can be measured on their performance and given credit for the added responsibility of security. This develops a sense of ownership for security and will ensure that the proper emphasis and time is dedicated to the security function.

As one continues through this process, one will see that one cannot get involved in one component of ISA development without touching on another. For example, while identifying security owners, one is discussing with them their responsibilities and initiating the user awareness component of the architecture. Additionally, it is necessary to discuss what procedures they currently perform related to security. For example, how is a new employee in the Accounts Payable Department set up on the system? What form do they use to request access? Who approves the access? How is access changed when someone moves from Accounts Payable to Accounts Receivable? These types of questions will not only identify the owners and security liaisons, but will also begin the process for defining appropriate security-related procedures. It also helps those individuals understand that it is truly their responsibility to perform these procedures. Once the procedures have been identified and documented, it will be necessary to determine if they are adequate or if they need to be modified to become more effective.

In identifying who is responsible for designating access to applications and who is responsible for the physical configuration of that access, it is appropriate and efficient to also look at the sensitivity of the information and application being assessed.

The Strategic Information Technology (IT) Plan

This chapter would not be complete without a discussion of the Strategic Information Technology Plan. The ISA is defined in the Strategic IT Plan, which is developed from the Strategic Business Plan. The responsibility for development of the Strategic Business Plan rests with executive management. The responsibility for development of the Strategic IT Plan rests with the CIO and the Director of the IT Department.

Before going much further, let us digress to a discussion of terminology: information systems (IS) versus information technology (IT). It is necessary to point out that some organizations use the term “Information Systems (IS) Department” to describe their systems function. Other organizations use the term “Information Technology (IT) Department” to describe the same function. Yet there are other organizations that have both an IS Department and an IT Department. Typically, these organizations separate

their systems department from the process of selection and implementation of new technology. This does not mean that the new technology is not considered a system. Until a system has been implemented, it is part of the developmental process and most likely requires significant resources and increased attention to ensure success. Technology implementation projects tend to be split from the day-to-day operation and maintenance budget of the IS Department. Companies are neither right nor wrong in how they choose to term their departments or functions. It can be indicative, however, of how large an organization's IS function is and how detailed the organization is in subdividing roles and responsibilities in the IS organization. Both terms — IS Department and IT Department — will be used interchangeably throughout this book.

Ten years ago, many organizations were happy not to hear or see anyone from the IS Department. That was because when they did, it usually meant something was wrong or something needed fixing. Transparency was key; and as long as IS kept everything running smoothly and stayed out of the way, all was right with the world. The IS Department was viewed as a necessary evil, a support function — key but not crucial to the business. This has changed. With the client portion of client/server sitting on most employee desktops, hearing and seeing IS professionals has become a daily occurrence. Through the use of technology, the IS Department has become the center of operations and key to the success of the business. Technology is viewed as the vehicle for achieving the business objectives of increased revenue growth, efficient production and performance, or decreased costs. The IS Department has become the means to the end through the use of technology.

The leading technologies that provide businesses with the capability to meet their business objectives are image processing, electronic data interchange (EDI), electronic commerce, communications technologies, workflow technology, area networks, collaborative computing and groupware, cooperative and client/server computing, intelligent agents, business process reengineering (BPR), mail technology, security, expert systems, Quick Response (QR), and telecommuting. Technology implementations are costly, and many implementations have failed because appropriate planning was either not performed or was not thorough.

The Business Plan is the basis for the organization's existence and includes a mission statement. This statement defines the business goals and objectives, which typically include references to revenue growth, increased production and performance, competitive advantage, increased quality and service levels, and decreased costs and time-to-market.

The Business Plan should also include a section on how the organization intends to achieve its goals and objectives. If it is through the implementation of technology, the Business Plan should refer specifically to the Strategic

Information Technology (IT) Plan. The Business Plan answers the who, what, where, when, why, and how of the business. This includes a budget for operations with a line item for the IS Department. The organization may choose to break out a separate line item to support the purchase, implementation, and maintenance of new technologies.

The Strategic IT Plan supports the business objectives as stated in the Business Plan. At a minimum, the Strategic IT Plan should be broken into six parts:

1. Introduction
2. Description of the IT Organization
3. Scope, Viability, and Modification of the Plan
4. Relationship to the Organization's Strategic Business Plan
5. Strategic Goals for Information Technology
6. Summary and Conclusion

Section 1 — Introduction — is an overview or executive summary that describes the background, origination, and intent of the document. Section 2 — Description of the IT Organization — should include a definition of the roles and responsibilities of individuals within the IT Department, an organization chart, and description of supporting staff, and a vision for the use of IT.

Section 3 — Scope, Viability, and Modification of the Plan — defines the scope of the document. An example of this section follows:

All information technology systems will be discussed, including information technology planned, developed, operated, and supported by the organization. The major goals and initiatives recommended by this plan are strategically significant to all business units of the organization. However, this document is intended to only reflect major institutional directions initially, with subsequent addition and modification to include corresponding plans of respective business units within the organization.

This strategic information technology plan is intended to be a "living" document with the primary purpose to serve as a communication vehicle across the institution. Strategic plans typically cover a time period of five years. Changes in technology occur so rapidly that it is not realistic for this document to remain static for that time period. Consequently, this document provides the baseline for IT planning and will be modified to reflect current priorities for information technology within the organization.

At its initial adoption, this plan will consist of essentially the primary goals, or initiatives, recommended and adopted at the institutional level. In the upcoming year, a more detailed action plan will be developed within the appropriate advisory groups and management levels for specifying how strategic institutional initiatives will be undertaken. On an annual basis, a revised information technology strategic plan will be presented to the executive management for review, along with a summary assessment from the CIO of how the organization is progressing in achieving goals or undertaking initiatives indicated in the plan.

INFORMATION SECURITY ARCHITECTURE

As this example indicates, the IT Strategic Plan is a document to reflect the direction for IT within the business. Supporting plans that address each technology issue should be developed in detail, to include planning for cost, selection, implementation, testing, maintenance, and consideration for security and control.

Section 4 — Relationship to the Organization's Strategic Business Plan — refers back to the Business Plan and provides a discussion of how the Plan is integrated with and supports the Strategic Business Plan. This section can also include a discussion of the industry's direction related to IT, including competition and the industry leader's use of technology to gain competitive advantage.

Section 5 — Strategic Goals for Information Technology — lists the specific objectives from the Business Plan that relate to IT. A sample table of contents from a Strategic IT Plan is shown in Exhibit 2-7; it lists the business objectives as Information Accessibility, Technology-Enabled Management, Staff, and Business Partners, Technology-Enhanced Business, Business Process Effectiveness, and Information Security Architecture. Subsections under each IT goal describe what must be accomplished to successfully meet the IT business objective.

Section 6 — Summary and Conclusion — provides a link to the specific and detailed plans that will support the Strategic IT Plan. For the Information Security Architecture business objective, this will result in an Information Security Architecture document that describes the eight components of the architecture and includes a security policy, security standards and procedures manual (SS&PM), security baseline assessments, user awareness program, compliance program, monitoring and detection program, computer emergency response plan, disaster recovery/business continuity plan (DRP/BCP), and a classification methodology.

The documents shown in Exhibit 2-8 are an integrated framework for achieving the goals and objectives of the business. The Strategic Business Plan is the foundation. It lists the goals and objectives for success in the business. The Strategic IT Plan supports the Strategic Business Plan by describing how technology will be used to enhance the business. Supporting and detailed plans for each business objective, including IT business objectives, define the step-by-step procedures for bringing the business to greater levels of success. An integrated framework provides the necessary links between the business goals and objectives, ideas and plans to achieve those objectives, and the step-by-step approach to accomplish the mission of the business.

The Strategic IT Plan needs to include the ISA as one of its objectives for the organization to operate effectively in a risk-reduced environment. Without an ISA, the organization may go on for several years without an incident.

Exhibit 2-7. Strategic IT Plan: Sample Table of Contents

Table of Contents

1. Introduction
2. Information Technology at XXXX Organization (Mission Statement)
 - 2.1 The CIO and Information Systems and Technology Roles
 - 2.2 The Information Systems and Technology Institutional-Level Organization
 - 2.3 Local Information Technology Support Staff
 - 2.4 The Evolving Information Technology Support Role
 - 2.5 A Vision for Information Technology Effectiveness
3. Scope, Viability, and Modification of This Plan
4. Relationship to the XXX Corporation's Strategic Plan
5. Strategic Goals for Information Technology
 - 5.1 A Corporate Goal: Information Accessibility
 - 5.1.1 Enhance and Extend the Network Infrastructure
 - 5.1.2 Ensure Appropriate Off-Site Network Access
 - 5.1.3 Ensure Effective Delivery of Information Technology Support
 - 5.1.4 Evaluate Services and Customer Satisfaction
 - 5.1.5 Establish Corporatewide Standards
 - 5.1.6 Effectively Manage and Distribute Servers
 - 5.1.7 Enhance Support of Library Initiatives
 - 5.1.8 Enhance Internal and External Communications
 - 5.2 A Corporate Goal: Technology-Enabled Management, Staff, and Business Partners
 - 5.2.1 Ensure Management and Staff Development in Technology
 - 5.2.2 Provide Appropriate Workstation Support for Management and Staff
 - 5.2.3 Promote Effective Research Computing
 - 5.2.4 Foster Technology Experimentation
 - 5.2.5 Provide Effective Information Technology Services for Clients
 - 5.3 A Corporate Goal: Technology-Enhanced Business
 - 5.3.1 Establish Appropriate Levels of Technology in Business Operations
 - 5.3.2 Ensure Availability of Information Technology Resources for Employees
 - 5.3.3 Engage the Corporate Community in the Use of Technology
 - 5.4 A Corporate Goal: Business Process Effectiveness
 - 5.4.1 Improve Efficiency of Operations
 - 5.4.2 Establish an Effective Data Warehouse System
 - 5.4.3 Replace Business-Process Software Systems
 - 5.5 A Corporate Goal: Information Security Architecture
 - 5.5.1 Establish an Organization that Supports the Security Function
 - 5.5.2 Establish Security Policies and Procedures
 - 5.5.3 Conduct Baseline Risk Assessments for Each Component of the Operating Environment
 - 5.5.4 Develop a User Awareness Program and Conduct Training for Employees and Individuals with Security Responsibility
 - 5.5.5 Develop a Comprehensive Compliance Program
6. Summary and Conclusion

INFORMATION SECURITY ARCHITECTURE

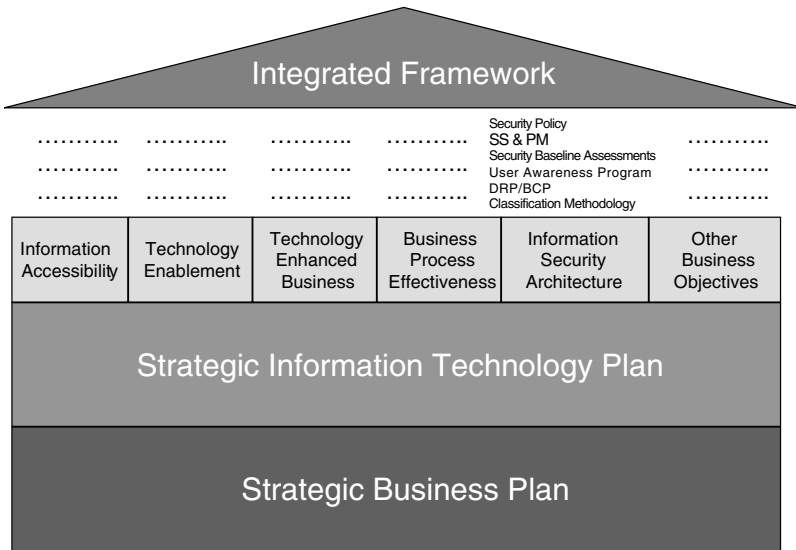


Exhibit 2-8. An Integrated Framework

When one does occur, however, the cost to the business could be much greater than the time and resources it takes to understand the risks, the operating environment, and the controls necessary to provide assurance that information systems and network resources are processing correctly, are safe from unauthorized use or access, and are available when needed.

Chapter Summary

An infrastructure must be developed to support the continuation of security architecture development and implementation. This infrastructure should include:

- Definition of the approval authority for all policies and resolution of security issues
- Definition of a Security Team for ISA Project development and the development, implementation, and dissemination of security policies, standards, and procedures
- Consideration for a full-time security organization tasked with leading the ISA project and performing ongoing risk assessment, security awareness, compliance, and security product implementations
- Establishing periodic meetings of all persons responsible for security, to include members of the Security Team; security liaisons, approval authority, representatives from all departments and business units, Legal, Human Resources, Help Desk, and application and network administrators

- Identification and documentation of the security responsibilities of those individuals listed in this chapter. (These responsibilities should be included in the job descriptions of each individual and those holding security responsibilities must be given performance reviews based on those responsibilities.)

Obtaining full-time staff for the administration of security is very difficult to achieve in the initial stages of ISA development. There are some very distinct and positive reasons for initiating the ISA Project with existing staff in a virtual team approach. The most significant reason is that it develops ownership for security responsibility at the department and operational level. Standards and procedures developed by those who must live by them is the most effective user awareness program that an enterprise can initiate. A virtual Security Team includes a single or small number of full-time security staff supplemented by an ad hoc group of non-security personnel from other departments to perform the functions of the Security Team. External professionals can also complement the Security Team. Once the ISA Project is in progress, it is important to keep executive management involved and aware of all the activities related to the development of the architecture. This awareness provides management with the ability to make informed decisions concerning appropriate security staffing requirements.

Finally, the Strategic IT Plan is the source document that brings security to the forefront through executive leadership and is integrated with the goals and objectives of the Strategic Business Plan. The organization must begin to recognize security at that level in the organization where appropriate resources can be allocated to implement security effectively. The ISA begins at the strategic level, through planning and support from executive management. The first step of the ISA is to include security in the goals and objectives of the Strategic IT Plan. This will ensure that the integrated efforts of the many individuals responsible for security throughout the organization are moving toward a common objective that is realistic, reachable, and appropriately supported by the key business leaders.

The ISA Project can last many months, depending on the amount of resources dedicated to the project. There are many deliverables related to the project, and it is very easy to lose focus on what you are trying to achieve. The ISA is a process and, through the development of that process, user awareness and understanding throughout the enterprise should be achieved. Those leading the ISA Project should be very organized and focused on obtaining this objective. The “Getting Started” subsection that follows provides tools in the form of worksheets and examples that offer the necessary structure to effectively initiate the ISA Project and provide appropriate project management.

Getting Started: Project Management

The most important aspect of initiating the ISA project is project management. Because of the distributed nature of roles and responsibilities and the many deliverables associated with the project, it is very easy for the project to become convoluted and lose its direction. Assigning tasks and expected delivery dates to each task will keep the team operating toward a common objective. It is important not to go into too many directions at once. Keep in mind that the development of the ISA is a process, and through this process one achieves security awareness at all levels of the organization. That awareness cannot occur over a two-week time period and it cannot be purchased from a consultant. It must be developed through active participation of all individuals within the enterprise. User awareness and the human element are the most important factors in security because it is the human element that can thwart even the most costly technical security tool.

The ISA project should be initiated in phases. The first phase is to define how the project will be managed. This includes setting up the Executive Committee for Security and the Security Team, explaining roles and responsibilities, gaining buy-in from both executive management for resources and the Security Team for their active participation, drafting a project charter that defines the scope of the project, and presenting the proposed ISA project to the Executive Committee for Security.

The project must be initiated and supported by upper management for it to be successful. Executive management participation in the project kick-off and correspondence to all employees from executive management to communicate the project as a corporate priority will set the stage for success. A letter from management to all departments should include a description of the ISA project so that employees are aware that security activities and information gathering is in progress (see Exhibit 2-9). The letter should address upper management's support for the project and request full cooperation of all departments and users. Exhibit 2-9 provides a sample letter used to initiate the ISA project.

Project sponsors typically include the CFO and the CIO. The project leader should be someone who can dedicate his full efforts to the ISA project. This is typically the Security Officer responsible for coordinating all security activities. As the project leader, it is suggested that the Security Officer develop a Project Charter to summarize the scope of the project and provide detailed management objectives and activities for each phase of the project. The sample charter in Exhibit 2-10 can be used as a guideline to develop a charter specific to a project. The charter should include a statement of business need and the approach, scope, resources, timing, and deliverables that are the outcome of the project. The charter provides the ability to measure if the project objectives have been met.

Exhibit 2-9. ISA Project Announcement Letter: Sample

September 1, 2004

To: See Distribution
From: Fred Grunner, CIO
Subject: Information Security Architecture Project

The purpose of this memo is to make you aware of the Information Security Architecture (ISA) Project that is currently in progress and to ask for your cooperation and assistance in gathering related information for this project.

In an effort to strengthen and standardize information security, Starcross, Inc., has initiated an internal project to develop an enterprisewide Information Security Architecture. The information systems and processes that manage proprietary manufacturing information are key targets for security breaches. Emphasis will be placed on developing controls to ensure confidentiality, integrity, and availability of all processes and information. The ISA will incorporate information into recommended security policies and procedures to be used as documentation for Starcross' information security requirements. In addition, the ISA will functionally combine technical and practical/cost-effective solutions with sound management practices to provide an adequate and appropriate level of security for other sensitive, critical, and proprietary information, information systems, and supporting computer resources.

The goals for the project are as follows:

- Develop information to be incorporated into security policies.
- Identify and document platform, operating system, database, and selected application security requirements.
- Conduct a risk assessment of the computing environment and connectivity into the network.
- Identify sensitive data transmitted across networks.
- Identify remote access processes and security requirements.
- Recommend potential solutions for security issues identified.
- Develop a high-level implementation plan.

The ISA Project Team has been formed and is made up of individuals involved with the project who may have ongoing security responsibilities. The purpose of the Project Team will be to document current practices and procedures, identify and report weaknesses, review and contribute to draft deliverables, develop and review draft policies and procedures, and assign ownership of security. Members of the ISA Project Team are:

- Bill Gernsey, Security Officer, ISA Project Manager
- Virginia Forsythe, Risk Management
- Max Hennessey, Human Resources
- Mike Compton, Internal Audit
- James Halloran, Network Services
- William Marlow, Customer Service (Help Desk)
- Jeff Paramount, Manager, UNIX Platforms
- Winslow North, Security Administrator
- Jean Barton, Application Development
- Beth Barstow, Manager, Mid-range Platforms
- Betty Rubble, Consultant, Enterprise Security Systems (ESS)

INFORMATION SECURITY ARCHITECTURE

Exhibit 2-9. ISA Project Announcement Letter: Sample (continued)

A wide range of departments will be contacted by members of the Security Team to set up interviews for collecting documentation and for identifying current practices and future requirements. Information already collected by other projects will be used to minimize duplication of efforts. Assistance in obtaining commitment for resources will be appreciated.

Exhibit 2-10. ISA Project Charter — Sample

Starcross, Inc.
Enterprisewide Information Security Architecture
Project Charter

September 1, 2004

Business Need

Starcross, Inc., is in the midst of an evolution in its computing environment — developing or acquiring new applications, integrating its mainframe heritage systems with distributed and multi-platform processing environments, and employing new technologies to meet business needs. Several trends are occurring in the manufacturing industry, many of which apply to Starcross, Inc., including:

- Using networking technology where physical location of end users cannot be assured
- Implementing integrated manufacturing systems to handle operational and administrative data across diverse and complex systems and networks
- Requiring access to applications on multiple types of computing platforms to support users' day-to-day activities, each platform requiring its own unique log-on ID and password
- Transferring easily and/or replicating data from production environments into end-user computing environments, with minimal involvement of information systems personnel
- Developing sophisticated PC-based communications capabilities that emulate a variety of device types
- Emerging recognition of the viability and value of remote access (i.e., dial-in and Internet) as a mechanism in the manufacturing environment

These dramatic technological trends, coupled with the equally dramatic business trends in the industry itself, result in great challenges to maintain the security, integrity, and availability of the vital information needed to make key operational, financial, and product development decisions. Conversely, more and more security solutions are being developed to address these risks.

Starcross, Inc., has initiated a project to develop and implement a comprehensive and flexible enterprisewide Information Security Architecture (ISA) for this new and evolving environment. Starcross, Inc., is a complex enterprise with multiple divisions, departments, and sub-organizational units and operates a heterogeneous processing environment with multiple platforms, networks, and protocols.

Exhibit 2-10. ISA Project Charter — Sample (continued)

The ISA must functionally combine technical solutions and practical/cost-effective solutions with sound management practices to provide an adequate and appropriate level of security that:

- Protects sensitive, critical, and proprietary information from unauthorized access, disclosure, or modification
- Protects information systems and supporting computer resources from accidental or deliberate loss, damage, or destruction
- Provides Starcross, Inc., management with reasonable assurance as to the integrity, confidentiality, and availability of information assets and computing resources
- Recognizes and adopts all federal and state regulations concerning the dissemination of copyrights, patents, and formulas

Approach, Scope, and Deliverables

Our approach will focus on the confidentiality of information and the functions, flows, processes, and applications specific to protected information and critical operating information. We will also focus on the network and its data flows and will perform a detailed assessment of data integrity and security for all Starcross, Inc., applications, connected servers, and workstations that are identified as having the greatest risk of loss. The deliverables associated with each task within our approach are specified.

Task #

Task

1. PROJECT KICKOFF MEETING

Initiate Planning Activities — We will work with Starcross, Inc., leadership to develop the project plan and governance structure necessary to guide the project for its duration. This task includes finalizing project scope and approach, identifying areas to be reviewed, and finalizing the project schedule.
 Committee Presentations — We will present an overview of the Information Security Architecture Project to selected committees within Starcross, Inc., to gain support and resources and to provide background information to key management.

Deliverables:

Finalized Project Charter and Schedule
 ISA Project Presentation

2. ARCHITECTURAL OVERVIEW — PHASE 1

The first project phase will allow the Security Team to gain the necessary architectural information to understand Starcross, Inc.’s environment, security risks, technology directions, and concerns relative to the processing environment and connectivity that will be reviewed. Team members will focus our inquiry to related and common aspects of the architecture, identifying security objectives as they are currently understood and as they should be implemented to achieve management’s security goals.

Obtain understanding of the processing environment and network architecture.
 Obtain understanding of systems management.
 Obtain understanding of security administration.
 Obtain understanding of new technology assessment and deployment.
 Obtain understanding of outage/threat response capabilities.

Deliverables:

Draft — Resource Ownership Matrix
 Documented issues and risks

INFORMATION SECURITY ARCHITECTURE

Exhibit 2-10. ISA Project Charter — Sample (continued)

Task #	Task
3.	<p>TECHNICAL AND ADMINISTRATIVE REVIEW OF COMPONENTS AND CONNECTIVITY — PHASE 2</p> <p>With the understanding gained during the first project phase, Team members will be prepared to begin the assessment of security controls for each component of the processing environment and its connectivity. Our assessment is structured in the form of a path analysis. For each component and its connectivity, Team members will identify the path used, devices providing security functions along the path, and the security controls that are available or used. The path analysis will include an identification of points of access authentication, authorization, administration, as well as monitoring and reporting. We expect that this activity should take 12 weeks. An analysis will be conducted to document the technical requirements for the networking environment and interface specifications needed to transmit data and images among user departments.</p>
4.	<p>Identification and Documentation of Platform, Operating System, and Database Security Requirements</p> <p>Obtain a high-level understanding of the component's configuration. Develop baseline security configurations for each component.</p>
5.	<p>Perform Dial-in and Dial-out Access Review</p> <p>Evaluate external connections and dial access. Evaluate network security features. Develop access path schematic.</p>
6.	<p>Assess Wide and Local Area Network Gateways</p> <p>Identify gateway controls. Identify gateway maintenance procedure. Identify threats to gateway implementation. Assess effectiveness of gateway controls. Develop access path schematic.</p>
7.	<p>Assess Current and Future Internet Connections</p> <p>Evaluate Internet controls. Develop access path schematic.</p>
8.	<p>Starcross, Inc., Connections to Business Partner's Networks</p> <p>Identify risk associated with peer connections. Identify controls available. Develop connectivity requirements. Develop access path schematic.</p>
9.	<p>Protection of Sensitive Data Across the WAN</p> <p>Identify special security requirements. Identify network resources used. Identify controls available to support security and confidentiality requirements. Identify other means available to support security requirements. Document analysis results. Identify security products and services/effective use of current resources. Develop evaluation criteria for any product evaluations. Complete analysis of services and products/effective use of current resources. Physical risk identification.</p>

Exhibit 2-10. ISA Project Charter — Sample (continued)

Deliverables:

- Access path schematics
- Draft audit workplans
- Proposed classification methodology

10. PROJECT REPORTING AND MANAGEMENT PRESENTATIONS — PHASE 3

Each of the previous reviews will result in a report that documents the environment and identifies issues and specific recommendations for that area, including suggested policy recommendations and solutions. The final deliverable will be a culmination of these reports and an overall assessment of risks, observations, and recommendations, including a suggested implementation plan. The suggested implementation plan will provide a prioritization of implementation activities based on the effort required and the potential benefit in terms of risk reduction that can be expected.

We will be prepared to provide a draft copy of the report for review by the project team. We will also be prepared to present our observations and recommendations to Starcross, Inc.'s management at the conclusion of the project.

Deliverables:

- Draft Information Security Policy
- Draft Security Standards and Procedures Document
- Proposed Information Security Architecture Implementation Plan

Key Milestones

The project will be completed over a 16-week timeframe. Critical milestones that will assist in the measurement of progress to date will be the following events/deliverables and corresponding targeted completion dates:

Formulate Project Team	May 16, 2004
Develop Project Charter	May 16, 2004
Refine Information Security Policy	May 28, 2004
Present Charter and Policy to Executive Committee for Security	June 5, 2004
Develop Resource Ownership Matrix	June 9, 2004
Develop Classification Methodology	June 11, 2004
Network Security Assessment	July 1, 2004
Baseline Security Configurations	July 10, 2004
Access Path Diagrams	July 15, 2004
Identify Security Issues	July 31, 2004
Draft Standards and Procedures Document	August 15, 2004
Develop Recommendations to Address Security Issues (Formulate Architecture)	August 31, 2004
Present Proposed Information Security Architecture to Executive Committee for Security	September 15, 2004

See the attached *Project Workplan* for further detail.

INFORMATION SECURITY ARCHITECTURE

Exhibit 2-10. ISA Project Charter — Sample (continued)

Project Sponsors and Information Security Architecture Project Team Members

This project will be sponsored by Fred Grunner and Charles Croft. Starcross, Inc., Security Team Members, in addition to the Project Sponsors, who will have a critical role in the development of an enterprisewide Information Security Architecture (ISA), to include:

<i>Project Sponsors:</i>	<i>Telephone #:</i>
Charles Croft, Chief Financial Officer	(123)123-1237
Fred Grunner, Chief Information Officer	(123)123-1238

<i>Project Team Members:</i>	<i>Telephone #:</i>
Bill Gernsey, Security Officer, ISA Project Manager	(123)123-2123
Virginia Forsythe, Risk Management	(123)123-2124
Max Hennessey, Human Resources	(123)123-2125
Mike Compton, Internal Audit	(123)123-2126
James Halloran, Network Services	(123)123-2127
William Marlow, Customer Service (Help Desk)	(123)123-2128
Jeff Paramount, Manager, UNIX Platforms	(123)123-2129
Winslow North, Security Administrator	(123)123-2130
Jean Barton, Application Development	(123)123-2131
Beth Barstow, Manager, Mid-range Platforms	(123)123-2132

External Security Systems (ESS) Engagement Team

This project will be supplemented by the following consultants from ESS:

Engagement Management:

Robert Heinz will maintain overall responsibility for the direction and delivery of this project.

Betty Rubble will serve as the external project facilitator to Starcross' Security Team and will be responsible for the overall coordination and delivery of services to executive management. Betty will also serve as primary contact for questions and project status updates.

Change Management Approach

As the engagement proceeds, should we encounter any potential revisions in the scope of this engagement, we will define the proposed engagement scope revisions for the Project Sponsors. Additionally, we will obtain approval from Project Sponsors prior to incurring any additional resources or expenses associated with the change in the project scope.

The ISA Project Team consists of the Security Team members. The ISA Project Team and the Security Team will be used interchangeably throughout the book. The project kick-off meeting should be designed to educate the participants on the purpose and structure of the ISA. The objective of the kick-off meeting is to co-develop expectations for this project and accomplish the following:

- Review in detail the Project Charter.
- Address project management.
- Co-develop team member responsibilities.
- Identify and gather appropriate documentation.
- Identify and schedule appropriate individuals for preliminary interviews.

Distribution of the letter (Exhibit 2-11) and kickoff meeting agenda (Exhibit 2-12) to the project team members will help them prepare for the meeting.

Exhibit 2-11. ISA Project Kick-Off Memo — Sample

Memo

Date: July 1, 2004

To: See Distribution

From: Bill Gernsey

Subject: ISA Project Kick-off Meeting

The Enterprise Information Security Architecture (ISA) Project kick-off meeting will be held on Friday, July 17, 2004. In this meeting we will review and discuss the scope of the work that is to be performed over the next 16 weeks. Phase 1 of this project will be performed over the next two weeks with the intent of gaining a sufficient understanding of the network, processing, and business environment to identify technical and business risks, and to evaluate the controls implemented for each of the connectivity types.

Winslow North will set up meetings between the ISA Project team members and Starcross departments to facilitate Phase 1 objectives. The following interviews have already been scheduled:

<i>Individual</i>	<i>Dept</i>	<i>Date & Time</i>	<i>Location</i>
Allan Harrison	Network Svc.	Monday, July 20 at 9:00 a.m.	22 North Lamont, 9th floor
Darvin Jones	Internal Audit	Monday, July 20 at 1:00 p.m.	Inland Park, 8th floor
Bill Harbison	Sales	Monday, July 20 at 2:00 p.m.	One North Adkins, 17th floor
Erin Halley	Network Svc	Tuesday, July 21 at 10:00 a.m.	22 North LaMont, 9th floor
Kevin Boch	Intn'l Trade	Tuesday, July 21 at 1:00 p.m.	One North Adkins, 18th floor
Tim Smith	Advantis	Wednesday, July 22, 10:00 a.m.	22 North LaMont, 9th floor
Barbara Hunt	Systems Dev.	Wednesday, July 22, 2:00 p.m.	22 North LaMont, 1st floor

During the meetings our object is to obtain an understanding of the following areas:

- Protection of Network Resources
- Administration of User Accounts
- Administration of Network Controls
- Network Standards & Procedures
- Network Performance Monitoring and Planning
- Network Backup and Recoverability

If there is any documentation available that supports the above areas, please bring it to the meeting.

Exhibit 2-11. ISA Project Kick-Off Memo — Sample (continued)

The following documentation will be needed:

- Organization charts
- Network diagrams
- Network management policies and procedures
- Security policies on physical/logical access controls of the network
- Network topology
- Network recovery plans
- List of applications transmitted over the WAN
- List of applications transmitted over the LAN
- LAN description
- Documentation on remote access procedures
- List of network management tools
- Documentation of performance standards
- Servers with applications listed
- Network-related decision papers on architecture or future implementations
- Internet addressing scheme
- Router filtering standards or documentation

If there are any documents that you feel are relevant to this project that are not listed here, please bring them to the meeting as well. I can be reached at 123-2123. Any documentation can be forwarded by Starcross internal mail. I also can be reached through the Starcross e-mail gateway over Internet using the following addresses:

billgernsey@starcross.com
bettyrubble@ess.com

Distribution:

Virginia Forsythe, Risk Management
Max Hennessey, Human Resources
Mike Compton, Internal Audit
James Halloran, Network Services
William Marlow, Customer Service (Help Desk)
Jeff Paramount, Manager, UNIX Platforms
Winslow North, Security Administrator
Jean Barton, Application Development
Beth Barstow, Manager, Mid-range Platforms
Betty Rubble, Consultant, Enterprise Security Systems (ESS)

There are many tools that can be used to simplify the information-gathering activities of this project. This book is designed to provide the reader with a starting point or baseline tool set of documents that can be modified to a specific project. It is recommended to develop an ISA database to record all activity and consolidate documents used to develop policies, standards, and procedures. Three large binders with dividers should be used to organize hardcopy information. One binder should handle all project management items, a second binder should contain a divider for each deliverable, and a third binder should contain a divider for each component of the operating environment. Suggested divider labels are as shown in Exhibit 2-13.

Exhibit 2-12. Kickoff Agenda — Sample

**Starcross, Inc.
Enterprise Information Security Architecture (ISA) Project
Kickoff Meeting Agenda**

The objective of the kick-off meeting is to co-develop expectations for this project and accomplish the following:

- Introductions
- Project charter review/modification
 - Project scope
- Project management
 - Timing and budget
 - Project status reports
- Review team member responsibilities
- Develop interview schedule

Administrative

Bill Gernsey	Phone (123)123-1234, Fax (123) 123-1233 E-mail bill.gernsey@starcross.com
James Halloran	Phone (123) 123-1232, Fax (123) 123-1233 E-mail james.halloran@starcross.com

It may be necessary to split each of the sections into a separate binder once the project progresses. Providing the project team members with a binder that includes dividers related to their responsibility will start them off organized and keep them focused on their particular responsibilities. For example, the Windows Netware Administrator may have a binder with both project management- and Windows-related dividers as follows: Project Management — ISA Charter, Security Contacts, Correspondence, Interview Schedule, Windows Administration — Network Diagrams, Sample Reports and Forms, Server Listing, Network Policies, Network Procedures, Network Standards, Vendor Contract, Scan Reports, Vulnerability Listing.

The purpose of the initial kick-off meeting is to get the Security Team organized and prepared to conduct the ISA Project. Interviews should be conducted for each component in the operating environment. The project should concentrate on one area at a time. It is suggested that because distributed computing with its emphasis on the network is known as an area of high risk and of particular concern to security, the network is a very reasonable place to start. Interviews should be conducted to gain an understanding of the processing environment and network architecture, security administration for that environment, new technology deployment, and outage and threat response capabilities. The example interview spreadsheet in Exhibit 2-14 will assist with the organization and scheduling of interviews.

Exhibit 2-13. Suggested Binder Labels

Binder 1 Project Management	Binder 2 Deliverables	Binder 3 System Components
Charter	Security Organization Chart	Remote Access
Budget	Security Ownership Matrix	Internet
Status Reports	Data Classification Methodology	Business Partner Gateways
Correspondence	Security Policy	Novell X.X
Security Contacts	Security Standards & Procedures Manual	Windows NT
Organization Charts	Vulnerabilities Reports	Windows XP
Network Diagrams	Audit Workplans	UNIX
Software/Hardware Listing	User Awareness Program	AS/400
Interview Summaries	Compliance Program	Oracle
Workplans	Year 2000 Plan	Lotus Notes
Sample Reports and Forms	Business Continuity/Disaster Recovery Plan	DB2 database
Current Policies, Standards, and Procedures	Computer Emergency Response Team (CERT)	E-mail
SAS 70 Reports	Business Continuity Planning (BCP)	Dunn & Bradstreet
References	Disaster Recovery Planning (DRP)	EDI

INFORMATION SECURITY ARCHITECTURE

Exhibit 2-15. Interview Template

Prepared by:
Reviewed by:

Starcross, Inc.

**Enterprise Information Security Architecture (ISA)
Project**

Interview	Name	Date:
	Title	
	Department	

Subject

OBJECTIVE

Material Overview

Topic — i.e., Processing Environment

Topic — i.e., Network Architecture

Topic — i.e., Internet Connection

Topic — i.e., Current Projects

Issues

Documents Required/Requested

Documents Received

Additionally, interviews should be documented so that team members can draw on interview summaries for the development of appropriate procedures. An interview template (Exhibit 2-15) will assist in standardizing the recording of interview information. With a team of individuals involved in a project, it is vital that all interview notes are documented and reviewed by team members. A Lotus Notes or similar database that can be accessed by all project individuals will ensure the dissemination of project information. It is important that a structure be developed for the filing of project information in the database and that document naming standards are developed to facilitate identification and use of the documents.

Another document that should be used for project management is a task tracking spreadsheet (see Exhibit 2-16). This spreadsheet lists all of the tasks related to the project, the person responsible for coordination of the task, the estimated time to perform the task, the estimated completion date, the actual completion date, and task review. This spreadsheet will

TASK TRACKING SPREADSHEET

TASK LIST	Responsible	Time to Complete in Hours	Target Date	Completed	Reviewed
Letter of Introduction to Departments		1	7/1/2004	7/1/2004	<input checked="" type="checkbox"/>
Project Kick-off Memo to Team Members		1	7/1/2004	7/1/2004	<input checked="" type="checkbox"/>
Develop Project Charter		6	7/5/2004	7/7/2004	<input checked="" type="checkbox"/>
Finalize Project Charter with Team		2	7/17/2004	7/17/2004	
Present Charter to Executive Committee for Security		2	7/25/2004		
Prepare Interview List		4	7/10/2004	7/26/2004	<input checked="" type="checkbox"/>
Gather enterprise documents for review		20			
Review organization charts		2			
Review network diagrams		2			
Review processing architecture		4			
Understand Impact of laws and regulations		8			
Define External Entities and Relationships to Starcross		16			
Conduct Interviews		80			
Draft Issues Discussion Document relative to architecture		40			
Develop Resource Owner Matrix		20			
Develop Security Contact / Liaison Appendix		4			
Draft / Modify Existing Information Security Policy		20			
Develop Other Security-Related Policies (Internet, e-mail etc.)		40			
Draft Information / Resource Classification Methodology		60			
Perform Computer Center Review		16			
Application Security - Placekeepers in S&P Documents		4			
Read Application Development Project Charter		2			
Develop Audit Workplans		80			
Internet Security Scanner Software - TCP/IP Addresses		16			
Schedule Axent ESM Review		16			
Schedule Bindview ESM Review		16			
Draft Security Standards and Procedures Document		600			
Develop Process Flows for Key Processes		40			
Develop Access Path Schematics		32			
Review Information Center Charter		2			
Develop / Modify System Access Request Form Templates		4			
Draft H/R Procedures - Notification of Termination		2			
Review Security Awareness Program Demos		2			
Develop Security Awareness Program		60			
Develop Compliance and Review Program		40			
Conduct Security and Awareness Training		16			
Conduct Status Meetings		40			
		Total Hours	1320		

Exhibit 2-16. Task Tracking Spreadsheet

help to budget resources for the project and can be used to demonstrate to management the resources required for effective security management.

The final project management document is the status report. The status report provides executive management with weekly correspondence regarding the direction of the project. It is another vital document that can be used to demonstrate the complexity and resource requirements of security administration in the distributed environment. Exhibit 2-17 is a sample status report that divides the report into three sections — issues, work in progress, and actions or decisions that are required. Keeping executive management informed of the issues that are uncovered as a result of the

INFORMATION SECURITY ARCHITECTURE

Exhibit 2-17. Sample Status Report

Starcross, Inc.

__ Internal Correspondence __ Pittsburgh Office

July 31, 2004

To: Charles Croft
Fred Grunner

From: Bill Gernsey
Betty Rubble

cc: Virginia Forsythe William Marlow
Max Hennessey Jeff Paramount
Mike Compton Winslow North
James Halloran Jean Barton
Beth Barstow

Enterprise Information Security Architecture (ISA) Project Status Report for 7/31/04

This memo is to document the ISA Project meetings and project status for the week of July 31, 2004. Attached is the revised Enterprise ISA Project Charter.

Interviews Conducted:

Allan Tose	Internet/Routers
Kevin Bates	UNIX (Engineering)
Bill Randolph	UNIX
	System Backups
Sam Houston	Windows NT
Johnson Henry	Help Desk

Performed automated scans of SC11 (UNIX) and SC 09 and SC 14 (Windows XP)
Attended the Cisco presentation on PIX Firewalls.

Issues:

The following list of issues was noted during the second week of field work. This is not a complete and comprehensive list as interview summaries and analysis of assessment reports have not been completed. This list is to give management a status of issues and an opportunity for discussing concerns prior to the issuance of a draft report. The issues are:

- Backup administration
- Termination/modification/review of system access
- Virus scanning of Internet/e-mail documents
- Transmission of sensitive data via Internet
- User awareness training

Work In Progress/Schedule:

The week of August 7 will be spent analyzing automated assessment reports and summarizing interview notes. We anticipate that the week of August 15 will be spent following up with interviewees and finalizing issues.

Exhibit 2-17. Sample Status Report (continued)

Actions/Decisions Required:

We anticipate that the vulnerabilities report will not be final by August 21. We recommend that a status meeting be held on Friday, August 21, to discuss issues and review the draft report with the Project Team. A follow-on meeting can be scheduled at executive management's discretion to present the final report to management.

The AS/400 review will begin on August 7, with Mary Roberts between 10:30 and 1:30. This review will be in conjunction with Internal Audit's annual review. The AS/400 review will be documented in audit workpapers separate from the ISA Project Report, unless specifically requested by management to include it in the Final Report.

project and asking them for decisions related to the project are extremely important to the project's success. Often, executive-level management is very busy with other projects and issues and cannot become hands-on with the ISA project. The status report provides key management with the ability to stay involved in the decision-making process related to the project. It is recommended that a status report be generated on a weekly basis.

Deliverables

It is important that while reviewing the Project Charter with the Security Team that you review the deliverables of this project. Those deliverables will help guide the activities of the Project Team. Those deliverables include:

- Enterprise ISA Project Charter
- Resource Ownership Matrix
- Information Security Policy — DRAFT
- Issues Discussion Document
- Baseline Security Configurations
- Audit Workplans
- Information Security Standards and Procedures Manual (SS&PM) — DRAFT
- User Awareness Program
- Compliance and Review Program
- Computer Emergency Response Program
- Disaster Recovery/Business Continuity Planning (DRP/BCP) Program
- Proposed Information Security Architecture

The Project Charter defines the project objectives, scope, resources, timing, and deliverables. It is important to gain agreement on the content of the Charter before beginning the project. This will ensure everyone is

INFORMATION SECURITY ARCHITECTURE

working from the same understanding. The second deliverable is the Resource Ownership Matrix. Discussion relative to this matrix by the Project Team will define project participants, their level of participation, and their responsibilities. The Project Classification Methodology is used by the data/resource owners to determine the level of protection required for the most important information and resources related to business objectives.

Many of these deliverables will be under development at the same time. It is important to designate one individual from the Security Team per deliverable as the person responsible for gathering information and pulling the deliverables together into a draft product. The Security Team can be broken into smaller groups to assist the assigned individual with completion of the deliverable. Work on each deliverable should be reviewed by members of the Security Team at each status meeting.

The Information Security Policy and the Issues Discussion Document are two deliverables in which all members of the Security Team will have significant input. If an existing Information Security Policy exists, it should be reviewed and modified as necessary. If a policy does not currently exist, it will be necessary to develop a baseline policy. Chapter 3 provides the process for developing policies, standards, and procedures, and example baselines.

The Issues Discussion Document is a very important deliverable that becomes the basis for security architecture decisions related to security programs, procedures, and technology implementations. It is the single source of all issues that are uncovered throughout security architecture development and during security baseline assessments. Its development should be initiated at the very beginning of the project so that all team members are aware of the type and format of input they are expected to provide. The document will consist of an executive summary that defines the background of the project, its scope, a definition of risk ratings, strengths identified, and overall conclusions. Exhibit 2-18 provides an example table of contents from an Issues Discussion Document.

The body of the report will be divided into chapters for each component assessed. Each section or chapter will include an overview of the environment, the methodology used to assess the environment, and a report of issues section. It is the report of issues section that the Security Team members will be required to develop. An example is shown below of an issue related to password parameters. Security Team members should be provided with this format so that they can begin to develop issues as they conduct interviews and assess components of the operating environment.

Password Parameters. *Issue:* User passwords are the first line of defense against unauthorized access to company systems. A review of the password

Exhibit 2-18. Table of Contents — Issues Discussion Document (Sample)**Table of Contents**

Executive Summary	1
LAN Assessments	2
Overview	2
Methodology	2
Windows NT LANs	4
Windows XP	5
Report of Issues	6
UNIX Security Review	10
Overview	10
Methodology	10
Report of Issues	11
LAN/WAN Gateway Review	13
Overview	13
Methodology	13
Routers	14
LAN Segmentation	15
Remote Access	16
Internet	18
E-mail	20
EDI	22
Business Partner Gateways	23
Report of Issues	24
Conclusion	25
Glossary of Terms	26
Appendix	27

files indicated that a number of user accounts have no assigned passwords. Accounts without passwords greatly increase the chances of unauthorized access to the system. Unauthorized users can readily gain access to accounts without passwords.

During our review, we noted that users on the system have passwords of five characters or less in length. Short password length results in less complex passwords and increases the probability that passwords will be compromised.

Also, we noted that user passwords are not changed on a periodic basis. As a result, the possibility of unauthorized persons gaining access to the company's system is increased as passwords tend to lose their integrity (e.g., become discovered or guessed) over time.

Risk: (High) If a user's account is compromised, unauthorized system access can be obtained and detection may be difficult because the account is valid.

INFORMATION SECURITY ARCHITECTURE

Suggested Action: It is recommended that all user accounts be assigned passwords. These passwords should be at least eight characters in length and should not be common words. The use of password phrases should be encouraged. In addition, the following password practices should be considered and, when practical, incorporated in the password section of the company's security policies:

1. Implement a proactive password checker to force good password selection as users change passwords.
2. Implement password aging for all general user IDs, and for all application IDs where possible.
3. Implement expiration dates on all user accounts.
4. Remove all guest accounts from the system unless they are absolutely required. If they are needed, use a restricted shell.
5. Password protect well-known accounts. Disable them if they are not necessary.
6. Change the passwords on every "default" account that came with the system and application software packages.

Security baseline assessments are performed to document and evaluate the adequacy of established controls, identify weaknesses and related business risks, and provide recommendations to strengthen current controls. The issues should be communicated to those individuals responsible for the maintenance and administration of the component. The issues should be documented in the Issues Discussion Document. The recommendations are intended as potential enhancements to the controls already in place. For purposes of discussion, risk ratings can be assigned to each issue. Suggested risk ratings are defined below:

- *HIGH* — Control concern. Issue should be addressed immediately.
- *MEDIUM*—Control issue for consideration by IS management to further evaluate risk.
- *LOW*—Informational. No action deemed necessary; continue to monitor.

Audit workplans can be developed and used to perform the security baseline assessments and can be used in the review and compliance component of the ISA. Compliance begins once security policies, standards, and procedures have been developed, communicated through a user awareness program, and implemented throughout the enterprise. The Security Standards and Procedures Manual (SS&PM) is developed from current procedures, the recommendations of the Issues Discussion Document, and industry best practices.

The proposed Information Security Architecture must combine technical solutions and practical (cost-effective) solutions with sound management practices to provide an adequate and appropriate level of security.

The architecture is a combination of the recommendations and solutions of the eight components:

- Security infrastructure/organization
- Policies, standards, and procedures
- Security baseline/risk assessments
- User awareness training
- Compliance
- Monitoring and detection
- Computer incident/emergency response
- Business continuity/disaster recovery planning (BCP/DRP)

Such a perspective provides a more consistent view of security services across the processing environment. It also provides a unique view of business security requirements and the services used by particular business functions. Solutions should be evaluated in terms of functionality, manageability, consistency, and availability so that the cost and benefit of any particular security approach will be evident.

Notes

1. The above information is from the Gartner Group, Inc., and was published by *CIO Magazine*, ©1998 CIO Communications, Inc., in the CIO.Com Magazine, <http://www.cio.com/forums/executive/description.html>
2. Taken from a controller job listing of the 5/8/98 issue of CFO Publishing Corporation.
3. Several of the functions listed above have been taken from an article in the September 1997 issue of *Preventing Business Fraud* entitled "Which Audit Committee Activities Do the Most to Prevent Fraud?".
4. Gartner Group, Administrative Application Strategies (AAS) Research Note, "Strategic Planning Assumptions on the Organizational Placement of Information Security," February 27, 1996.
5. G. Lynch, Information Security Strategies Research, "The Metamorphosis of the Information Security Organization," Gartner Group, January 29, 1996.

Chapter 3

Security Policies, Standards, and Procedures

Introduction

This chapter discusses the requirements, development, and implementation of security policies, standards, and procedures. Uniformity in applying security safeguards requires the development of written guidelines for the secure configuration of operating systems, databases, applications, Web servers, routers, and other software and hardware. To be effective, well-directed workgroups (e.g., as the Security Team) must develop technical security guidelines; this should involve the individuals affected by those guidelines.

Learning Objectives

When one has finished reading this chapter, one should be able to:

- Understand what a policy is and how it should be structured.
- Understand the necessary content of a corporate security policy and policy acknowledgment form.
- Understand the concerns and issues related to corporate e-mail, privacy, and monitoring, and be able to develop a comprehensive e-mail policy that protects the organization.
- Understand federal laws related to monitoring and disclosure of corporate e-mail.
- Understand the risks of Internet access and be able to develop an Internet policy.
- Understand what a standard is, identify the security standards organizations, and know where to look for security standards on the Internet.
- Understand what a procedure is and know what security procedures must be developed for the organization.
- Define these key terms:
 - Security Policy
 - Security Standard
 - Security Procedure
 - Request for Comment (RFC)

Policy is designed to inform all individuals operating within an organization of how they should behave related to a specific topic, how the executive management of an organization feels about that topic, and what specific actions the organization is prepared to take related to that topic. In this case, we are specifically addressing information security policy. An Information Security Policy should describe, in written format, what executive management is trying to achieve, the policy objective. It should also include the policy scope, responsibilities, and management's intention for implementing it. The Security Policy addresses security activities that include designing controls into application systems, establishing user access privileges, performing risk analysis, conducting investigations of computer crimes, and disciplining workers for security violations.

Standards consist of a specific set of rules, procedures, or conventions that are agreed upon between parties in order to operate more uniformly and effectively. For example, if every department were to choose a different e-mail application, it would be very difficult to communicate between departments because there is no set protocol or agreement on how or what to purchase or how to interoperate. Another example is that if everyone in an organization wrote a letter with no guidance on how corporate letters are to be formatted, some of the letters would probably turn out pretty nice and others might be embarrassing to send. Standards set a level of expectation that must be reached or exceeded to fulfill one's obligation or responsibilities. Standards have a large impact on the implementation of security. When standards have not been taken into consideration related to technology implementations, it may impact the amount of energy or support required to meet the enterprise's security objectives. This will have a definite impact on both cost and the amount of risk. Policies answer the who, what, and why for a specific topic.

Procedures are plans, processes, or operations that address the specifics of how to go about a particular action. They enable the transfer of knowledge between individuals who perform the same job, cover for each other during periods of absence, or allow for a more knowledgeable and smoother transition during permanent staff changes. Procedures should reflect best practices that have been established. They should also reflect improvements that have been made to a process to provide for efficiency by virtue of the repetitive nature of performing a specific task. Procedures are also guidance but typically answer the more detailed questions of where, when, and how.

This chapter is designed to assist the reader in developing and implementing policies, standards, and procedures more effectively. Many organizations have policies, standards, and procedures but they may be unwritten. Unwritten policies create confusion, are difficult to enforce, and create inconsistent implementation of controls. It is very difficult to test something

that is undocumented for effectiveness and compliance. In addition, it has been set as a legal precedent that companies must show or prove due care when enforcing policies, in which case they have made an effort to be in compliance, at a minimum, with industry security standards. From a legal perspective, enterprises must be prepared to show that they have communicated to their employees, users of their systems, and business partners appropriate use of those systems and resources, as well as appropriate ways to effectively protect their business, information, and resources, from damage, theft, destruction, or unauthorized access. This will minimize the risk of legal liability due to negligence and breach of fiduciary responsibility.

Policy is often developed as a regulatory obligation. Federal, state, and local governments are required to abide by and develop policies by which to govern. The healthcare industry is required to develop policies related to patient medical record confidentiality. Banks are accountable for their operations according to the Federal Financial Institutions Examination Council (FFIEC) and the Office of the Comptroller of the Currency (OCC), and publicly held organizations must answer to public accounting firms for their operational procedures and policies. Developing policies, standards, and procedures because one is required is not good enough. One must develop and implement policies effectively to meet the enterprise objectives.

Policies are used as a communication mechanism between executive-level management, employees, and system and information users. They establish the understanding that management supports certain behavior and means business when their directives are not followed. This provides credibility, flexibility, and support to information security efforts on the part of other individuals throughout the organization. Policies also establish the basis for disciplinary action and legal prosecution if necessary. They should be written in a clear and concise manner that reduces the amount of misinterpretation. This will enhance the performance review structure and assist in any legal actions that would arise from noncompliance. Policies should not undermine the way people really work. They should be based on educating users, not scaring them. Scare tactics tend to deter users from reporting problems such as compromised passwords and viruses.

This chapter provides baseline policies that can be used as a building block for developing specific policies customized to one's enterprise. Many organizations have tried to implement policies from a book or from another organization without making appropriate changes relative to the specific environment of the enterprise. Policies will be most effective if the Security Team, as a part of their responsibilities, reviews a baseline policy and provides input to modify it and make it reflect the culture and attitude of the organization and the technology represented in the processing environment.

INFORMATION SECURITY ARCHITECTURE

Again, this develops a sense of ownership and pride in the policy, and it is much easier for the Team to implement and enforce when it is something they have personally contributed to and produced. If policies, standards, and procedures do not already exist, it is the Security Team that develops them in draft form. This is because they have the technical knowledge related to the processing environment and the security requirements for that environment. The Executive Committee for Security or the governing body that performs executive-level decision making must perform the final review and approval of all security-related policies. Executive management must provide its opinion and support for the implementation of the policy. This can only be accomplished if the Committee understands the level of effort and support required to carry out those policies.

To develop security policies and procedures, one must first look at what one is trying to protect. This was discussed in Chapter 2 by taking an inventory of all the applications, operating systems, databases, and networks that the enterprise has in its operating environment. One then determines who is responsible for all of those components by developing the Resource Ownership Matrix (see Exhibit 2-6). Once responsibility has been determined, the best person to place a value on the information or resource is the owner of that information or resource. The resource owner must then look at the resource from a confidentiality, integrity, and availability standpoint and determine how to protect the resource in a cost-effective way based upon its value to the enterprise. Threat and realistic risk are also a necessary component. What must the resource be protected from, and how likely is it that the threat to that resource will result in loss or damage? This type of analysis provides an understanding of calculated risk.

Often, a qualified understanding of the level of risk has already been determined before standards and procedures are developed. Component 3 of the ISA is security baselines and risk assessments (discussed in Chapter 4). Because of audit requirements, these are frequently performed before policies, standards, and procedures have been defined. By the time an enterprise makes the decision to develop an ISA, the decision is based on a level of risk already known either through security baseline procedures, a financial audit review, or an incident that has already occurred and provided qualification of the risk.

In reality, policies, standards, and procedures should be reviewed continuously, and improved every time a weakness is found. Risk assessment is also a continuous function because the distributed computing environment is always changing. There is no set order for developing the components of the ISA because the ISA is an integrated process. The first three components — (1) security organization/infrastructure development, (2) policies, standards, and procedures, and (3) security baseline assessments — can be performed in any order or simultaneously, given resource availability

and still result in an effective architecture. The primary success factor is that they are all eventually developed and any weaknesses, changes, or issues discovered are used to improve the security process by modifying the policies, standards, and procedures. Chapter 4 details the security baseline activities for the most common components of today's processing environments. The last five components — (4) user awareness and training, (5) compliance, (6) monitoring and detection, (7) computer incident/emergency response, and (8) disaster recovery/business continuity planning — do not make sense to implement until the first three components are under way.

The Information Security Policy

The Information Security Policy should be short, easy to read, and unambiguous. If the policy is too long, users and employees will not read it. The policy should also be presented during security awareness and training sessions. It is more likely that it will be absorbed if it is presented in a light, funny, and interesting manner. If users are expected to read it on their own, it is a given that they will not. A digested version of the policy can be developed into a Security Policy Acknowledgment Form that the users are required to read and sign upon employment at the enterprise and prior to receiving computing assets. It is recommended that the acknowledgment form also be read and signed on an annual basis so that all users are reminded of their responsibilities to protect the confidentiality, integrity, and availability of the information and processing resources that they are privileged to use during the execution of their duties. Reading and acknowledging the Information Security Policy should be tied to a user's ability to gain a log-on ID and access privileges.

All well-developed policies contain the same common elements. Those elements are:

- An introduction or background on why the policy is necessary
- The statement of policy: the objective or what management is trying to achieve through the establishment of the policy
- The approval authority
- The authors
- References to other policies and regulations
- Compliance measures
- Consequences for violations
- Date of the policy

Two other areas that are typically included in an organization's general policies and procedures manual are a process for requesting change to the policy and a process for requesting exceptions to policies. These processes need not be included in each policy, but should be defined as their own procedures. Policies must be reviewed on a periodic basis to see if

INFORMATION SECURITY ARCHITECTURE

they should be modified or expanded to meet a changing organizational or operational environment. It is also important that directives of the policy are disseminated throughout the enterprise, and that department management ensures that the employees for whom they are responsible are aware of their rights and obligations under the policy.

The sample baseline policy in Appendix A-1 includes all of the common elements listed above, as well as the security responsibilities defined in Chapter 2. It is necessary to modify any security policy to the organizational structure, corporate culture, and technology environment.

One can provide policies to employees and users but it is difficult to validate that they have read and understood them. When policies are particularly lengthy and important, it is more effective to conduct a training class or awareness session to explain this importance through videos, stories, or other mechanisms that get the attention of the users. This is discussed further in Chapter 5 — “Security Awareness and Training.”

Information Security Policy Acknowledgment Form

A one- or two-page summary of the Information Security Policy that defines the user’s specific responsibilities should be signed at the beginning of employment and on an annual basis to remind them of their responsibilities. This signature can be used to validate that the user has been informed and understands his or her responsibilities. The Information Security Acknowledgment Form in Appendix A-2 defines what the user is to protect, the scope of resources, what his or her responsibility is to protect the resource, and an acknowledgment statement of the user’s understanding. This form should be reviewed by the Human Resources Department to ensure that it is within the guidelines of other enterprise policies and by the Legal Department or legal representation to ensure that it is legally binding and any punitive statements are enforceable.

Network Usage Policy

Other policies that relate to the protection of resources are the E-mail Policy, Internet Policy, and a new requirement is the E-Commerce Policy. As one can see, all of these security policies relate to the use of networks. An umbrella network policy could cover all of the topics necessary in network operation and usage but users need to have their responsibilities clearly defined for each specific topic. It is important to try not to do too much with one policy and lose the attention of the target audience.

The Network Computing Policy in Appendix A-3 covers network computing, electronic mail, and network security. It was taken from an Internet search and was described as “the mother of all Net usage policies.” That is because it is very specific to prohibitive behavior. Many organizations do

not want to seem militant in the communication or enforcement of their policies and requirements and will tone down the verbiage used in the policy. They do not want their employees to feel threatened or foster the indication that there is a lack of trust. Problems can arise, however, if the idea of instilling “trust” within the corporate culture is not appropriately balanced with the idea of protecting one’s assets and meaning business in doing so. A very real example follows.

INCIDENT: A manufacturer of a very well-known cooking product began as a start-up in the garage of a very small town. Many of the employees were from the local neighborhood and had been at the company for more than 20 or 30 years. Eventually, the company grew into a major manufacturing plant that was renowned internationally for its product. The company had patents on a specific metal annealing process and eventually implemented very costly and highly technical robotics to perform this process. This manufacturer was now stocking its products on the shelves of all the major retail chains. Because of the trust for its employees and its very simple beginnings, executive management felt that policies, especially those related to security, would be offensive to their workforce and signify that there was a lack of trust. There was no security policy and little separation of duties. Strong, restrictive policies such as the Network Computing Policy in Appendix A-3 would only serve to offend many of the employees in an environment where trust and loyalty had been cultivated through years of service. In this case, user awareness and training needed to be conducted for executive management so that they could understand the risks they were accepting to maintain that trust. Training needed to be conducted for the employees so that they understood the vulnerabilities of the operating environment and the need for protection of their assets. A policy targeted to this environment should be worded carefully and with few statements regarding punitive enforcement.

The Network Computing Policy in Appendix A-3, submitted by Michael Spindeler at mspin@halcyon.com, is listed because it is comprehensive and most restrictive. It is also written plain and simple and is very directed toward the reader. The way it is written entices the reader to continue to read because it is very pointed. It is not recommended that such a policy be implemented as is. It is a very good starting point that should be tailored to an organization’s culture and operating environment. This policy also has a place for signature and date to verify that the individual has been told of his responsibilities. This will support the enforcement of actions necessary if the policy is violated. The following section is specific to e-mail.

E-Mail Policy

The introduction of e-mail into the enterprise allowed departments and workgroups to establish communication to interact more efficiently. At its

advent, e-mail was sometimes implemented disparately throughout departments because of the lack of standardization in information systems. Many departments and divisions had the option of implementing systems specific to their group. Eventually, the barriers of ad hoc e-mail systems forced replacement with enterprise systems that were centrally managed and controlled.

E-mail has introduced efficiency into the work environment for both internal and external communications. Professor Palme of Stockholm University has researched and written a book on the subject, entitled *Electronic Mail*. In that book, Palme states that it takes 30 minutes to write the average business letter and more than 20 minutes for the average business telephone call. This does not include unsuccessful attempts to reach an individual by telephone. The average e-mail takes just under five minutes to produce. Along with this efficiency come the risks that must be considered and addressed. Managing and securing an enterprisewide e-mail system requires knowledge about the Internet and Internet security, encryption standards, international, federal, and state laws regarding privacy and electronic communications, policy development, and user awareness.

Now that e-mail has spread outside the bounds of the enterprise and one can communicate electronically with other organizations, it is even more important to establish policies and procedures for the appropriate use of this communications medium. Employees feel that they are somewhat anonymous while sitting behind their computers. It is important to make them understand that they represent the company, and any communication from corporate owned resources is tied back to the owner of those resources. For example, their message has the corporate Internet or TCP/IP mail server address and any return e-mail must come to the enterprise mail server. When Bill Gernsey sends e-mail, his address before it is translated at the mail server and as viewed by external entities is bgernsey@starcross.com. Messages sent via the corporate mail server typically identify the enterprise. Inappropriate messages would reflect negatively on the enterprise and can cause liability concerns.

An e-mail message is less expensive than a phone call and can be sent very quickly and easily and without interaction from a secretary, mail clerk, or even getting up from one's desk. This contributes to the false sense of privacy that users have when sending e-mail messages. Users should be aware that e-mail produces a written record of their communication that can be legally intercepted and reviewed by the enterprise. Writing a letter on company letterhead, interacting with a secretary to format and print the letter, and filing a memo or letter in the client folder are all actions that give us time to think about what we are communicating and how we will be perceived. The use of e-mail eliminates the thoughtfulness that goes into the preparation of a formal letter and users are less likely to think

about what they are saying or how they will be perceived before sending an e-mail.

The e-mail policy should be designed to protect business partners' interests, client information, the employee from himself, and the enterprise from liability. The most sustainable and productive policies are those that give appropriate consideration to the employee's expectation for privacy and also provide responsible procedures for conducting maintenance and monitoring as warranted in protecting the network and applications.

There are several laws that can be used defensibly to protect the enterprise in cases involving e-mail privacy, wiretapping, and keystroke logging. Most specifically, the Electronic Communications Privacy Act (ECPA), 18 U.S. Code Sections 2501 et seq., 2701 et seq., and 2510 et seq., governs unauthorized access to and disclosure of electronic mail messages. The ECPA prohibits the use of electronic or mechanical devices to eavesdrop on telephone and in-person communications. The ECPA does not, however, limit the policies that an enterprise can develop for the use of company-owned resources and applications in the workplace. E-mail is an enterprise asset and, as such, is under the jurisdiction of the enterprise. Under the laws stated above, consent by only one individual, either the sender or receiver, is required to access private e-mail. As a part of the E-mail Policy, the enterprise can make consent of access to private e-mail a condition of the use of this application. If this is the case, a signature indicating consent would best protect the company against violation of e-mail privacy laws. It is necessary to understand the state laws regarding electronic monitoring. Some states such as Pennsylvania, California, and Louisiana prohibit eavesdropping or intentionally recording confidential communications without the consent of all parties to the communication.

Additionally, the enterprise is responsible for protecting the security of the system and, in the execution of those duties, is permitted to monitor system traffic in real-time that contains e-mail messages. The wiretap statute allows the interception of messages by a company with equipment and procedures used in the ordinary course of its business (i.e., the protection of company assets and applications or system maintenance procedures). Banners should be used to inform anyone accessing the network and systems that they are subject to monitoring. The following banner statement should be shown at log-in and is a recommendation from the Department of Justice to ensure that the monitoring entity is not in violation of the ECPA:

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring for the purposes of maintaining a secure system and performing system maintenance, the activities of authorized users may also be monitored. Anyone using this system

INFORMATION SECURITY ARCHITECTURE

expressly consents to such monitoring and is advised that if such monitoring reveals evidence of criminal activity, system personnel will provide the evidence of such monitoring to law enforcement officials.

Employees use the e-mail application as a representative of the employer. As such, the employer, who authorizes the use of the application and that users send messages on the employer's behalf, has the authority to consent to the disclosure of the message content. Employers must protect themselves from liability suits that include defamation, harassment, discrimination, copyright infringement, and discovery. In discovery, the courts may require enterprises to have their e-mail searched for specific correspondence. These types of searches are becoming more common and can reveal damaging evidence against the enterprise.

Retention policies are specifically targeted at limiting how long backups of e-mail are retained. The more that is retained, the more costly a search can be at the employer's expense and the more likely something damaging may be found in e-mail during those discovery searches. It is very expensive to store and maintain this information. Companies must be careful in making promises of privacy to the users of the e-mail system because they may be required by contracts or discovery demands to turn over company records. Disclose to users in the E-mail Policy that there is the possibility that e-mail records may have to be disclosed to third parties due to litigation or contract obligations and there is no promise of privacy.

Recognize that it is difficult to enforce enterprise policies with contractors, consultants, or external entities that are communicating through e-mail to employees. There are additional considerations made for monitoring when e-mail service or networking is outsourced because the enterprise is not the owner of the system. Be sure to check with the outsourcer on its policies and procedures related to monitoring and take them into consideration when preparing the enterprise e-mail policy.

The e-mail policy should cover several areas, including:

1. The purpose of the e-mail system
2. Confidentiality and privacy issues and how to protect sensitive information through the use of encryption, if encryption is available, and what the use of encryption is limited to
3. The limits of personal use of the e-mail system, which can include business use only, incidental personal use, or unlimited personal use
4. Procedures for communicating with individuals outside the enterprise (i.e., business partners, customers, vendors, consultants, etc.)
5. Backup and retention of e-mail files
6. Restrictions relating to communications or information provided to corporate entities, business partners, or customers in other countries

7. System monitoring, which can include no monitoring, monitoring for business purposes, or monitoring for cause or legal purposes
8. Access and disclosure of messages can include no access without consent or unless required by law, access for cause under appropriate procedures, access and disclosure for any business purpose by authorized individuals, notification after the fact for any access or disclosure without consent
9. Penalties for noncompliance to the policy
10. Management's intent to enforce penalties

Appendix A-4 shows an example of an E-mail Policy. In this policy example, encryption of messages was not used as an option because it is assumed that the enterprise does not have encryption capability. Many enterprises do not. In this case, it is best not to transmit sensitive and confidential information over the e-mail system. Courier and registered mail are the most likely alternatives. If encryption is a capability that the enterprise has, then the policy should state specifically what types of documents should be encrypted and limit encryption to only those documents.

Encryption is a double-edged sword. If an employee encrypts proprietary documents that he is stealing and selling to a competitor and sends those documents over the network, the enterprise will be unable to detect through monitoring that inappropriate activity is occurring. However, encryption architectures usually include a mechanism for key recovery. If an individual is suspected of stealing information, transmissions can be captured and decrypted using the keys stored for key recovery.

The enterprise should also avoid the idea of encrypting everything. This most likely will have a performance-related impact on the network and goes against the primary objective of cost-effective security and allocating resources to protect only that which requires protection. Specific controls related to e-mail are defined in the "Procedures" section of this chapter.

Internet Policy

The Internet and E-mail Policies are related because e-mail is typically sent over the Internet. They should, however, be separate policies for two reasons: (1) length and (2) usage. Making a policy too long will cause the reader to lose focus and attention on what is to be conveyed by the policy. Additionally, e-mail is a service provided through Internet access. If e-mail is the only service being provided by a mail server through Internet access, the Internet is relatively transparent to the user. For users, the E-mail Policy will cover the security concerns and appropriate use of e-mail and the Internet Policy will probably not be necessary. When other Internet services are used, such as the transfer of files (FTP), the ability to log on remotely to a host at another location (Telnet), research capabilities

INFORMATION SECURITY ARCHITECTURE

through searches of Web sites and remote hosts, and establishing bulletin boards, it will be necessary to establish an Internet Policy.

Internet Risk

There are significant risks related to providing a network connection from the internal network of the enterprise to the Internet. The risks include:

- Lack of governance of the Internet
- Potential access to internal information
- Unproductive use of employee time
- Destruction, downtime, and maintenance costs due to viruses
- Vulnerabilities from competent, technically proficient yet destructive hackers
- Misinterpretation of company philosophies and practices
- Legal liability to the enterprise for misuse of Internet services such as e-mail or chat rooms

Because it is a massive network of connected hosts, no one particular organization owns the Internet. Any enterprise that connects to it is responsible for managing, controlling, and securing its connection and Internet usage. Internet users and several organizations provide self-governance of the Internet. A few of those organizations are the Internet Architecture Board (IAB), the Internet Engineering Steering Group (IESG), the Computer Emergency Response Team (CERT) Coordination Center, and the Internet Engineering Task Force (IETF). These organizations have written standards for the appropriate use and secure operation of the Internet, but there is no one group to enforce those standards. Internet user groups also provide appropriate use monitoring to some extent. Those who violate the semi-formal standards suffer backlashes from users, hackers, and user groups. An example of this is those who send unsolicited e-mails or advertisements or “spam” e-mail over the Internet. Users of the Internet will band together and respond to flagrant abusers by shutting down their Web sites or responding in-kind by flooding the abuser’s connection with junk messages. Spam e-mail has spurred the drafting of several bills that would make it illegal to send unsolicited bulk or junk e-mail messages or faxes.

An Internet connection can provide access to an enterprise’s internal information and processing environment by individuals external to the enterprise. These include customers, vendors, business partners, competitors, and ne’er-do-wells. It is very difficult to enforce enterprise policies for individuals outside the legal jurisdiction of the enterprise. Displaying banner statements upon log-in will notify external users of restrictions on access and appropriate use of resources. Firewalls will act as a filter of services not permitted and make it more difficult for those not authorized to penetrate the system.

Internet search capabilities provide individuals with the ability to quickly search thousands of databases for a topic of interest. This can increase an employee's efficiency in performing his or her job. On the other hand, there is so much information out on the Internet that an employee can become easily distracted with daily news, horoscopes, games, stock quotes, and e-mails to friends. This can be very unproductive for the enterprise. Many companies that monitor their Internet access to determine employee productivity have found thousands of hours wasted on non-business-related Internet use. This can be controlled through development and dissemination of Internet policy, user awareness, usage monitoring, and implementing filters that restrict access to certain sites.

Viruses and Trojan horses can be propagated throughout the enterprise through files downloaded on the Internet. Trojan horses are programs that appear to be harmless but represent destructive programs triggered to execute upon a certain activity or timeframe and can crash or erase a hard drive or cause other irreparable damage. Internet policy should include proper procedures for downloading files. Some firewalls can open and scan incoming files for viruses; however, this can create a bottleneck if Internet usage is high. A standard procedure is to provide a separate server where all files are downloaded and scanned.

The Internet is a breeding ground for illegal electronic activity. There are many Web sites that share techniques on how to break into certain sites, businesses, or systems. There are also very many technical individuals whose only hobby, profession, or interest it is to penetrate the computer system security of unpopular companies, new versions of operating systems, or sites that tout that they are not penetrable. It is important to understand that no system, site, or enterprise is "not penetrable." Any individual with the technical capabilities, resources, and knowledge regarding an enterprise's operating environment can gain access to that environment. The objective of the enterprise should be to provide enough deterrence and have effective monitoring built into the security architecture to detect intrusions as they occur and minimize damage to the organization.

Another risk includes misrepresentation of company philosophies and practices by employees publishing their personal opinions on behalf of the enterprise on bulletin boards, chat rooms, or other avenues of communication on the Internet. This also relates to e-mail. Many lawsuits have occurred against enterprises because of inappropriate humor, sexual harassment, bias, prejudice, derogatory, inflammatory, obscene, or threatening messages received over e-mail or through Internet communications. The only control for this risk is policy dissemination and user awareness training.

Process for Change

The Internet changes the way an enterprise does business. People are often resistant to change, especially when the changes are unexpected. Many of the support processes of electronic business will need reengineering. Inefficiency may occur because employees insist on continuing to do business the old way instead of embracing a new initiative. There will also be cultural changes that must be conveyed ahead of time to employees. Communication between management levels becomes easier and less formal, impacting the decision-making process. Information received through the Internet is often assumed by users as a valid source of information. This can have a significant negative impact on the enterprise if false information is used or disseminated within the enterprise. Prior to the use of e-mail and the Internet, departments kept their information under tighter control. Electronic storage and the ease of transmission have encouraged a more open environment, prompting cooperation and information sharing. This ease of communication can heighten productivity and efficiency as well as facilitate the distribution of maleficent information quickly throughout the enterprise.

The Internet Policy can be used to lay the groundwork for change in the enterprise. The changes are critical and often go unnoticed until the enterprise begins using Internet technologies for normal business operations. Changes will occur with the business processes; the use, storage, and elimination of paperwork; the number of people requiring access to information; decision making; and the structure of the organization. These organizational changes and cultural shifts, which generally occur within six months of Internet usage, must be managed through policy to achieve the desired benefits of Internet access. A sample Internet Policy is shown in Appendix A-5.

The sample policies in this chapter are designed to give the reader an idea of the format and content of security policies. These policies can be modified to the organization's specific operating environment. They should be reviewed by a representative from the Legal Department to ensure that they are enforceable and they should be approved by an Executive Council or Committee.

Policies should be made available to each individual within the organization. Intranet Web sites are becoming very popular in larger organizations to disseminate policy as well as other information of interest. Security policies should be presented at new employee orientation, and employees should be given appropriate time to read the information and sign acknowledgment forms. Policies should be revisited at least annually through user awareness and training sessions, e-mails to employees, and newsletters. They should also be reviewed and updated annually taking

into consideration new technologies, and changes to the business and the operating environment.

Security Standards

Standards are a specific set of rules, procedures, or conventions that are agreed upon between parties in an effort to operate more uniformly and effectively. There are many standards for all industries: the way electrical outlets are designed, plugs for computers, electrical currents, and tops for coffee cups. Security standards ensure that individuals operate consistently to minimize risk and to make administration of systems and networks more efficient. As stated previously in this chapter, standards set a level of expectation that must be reached or exceeded to fulfill one's obligations or responsibilities. Standards have a large impact on the implementation of security. When standards have not been taken into consideration related to technology implementations, it may impact the amount of energy or support required to meet the enterprise security objectives. This will have a definite impact on both cost and the amount of risk.

How do standards make operations more efficient? Let us go back to the e-mail example. If there are three different e-mail packages within an organization, there typically will be three different administrators for the different packages. User awareness and training classes must be developed for all three sets of applications. Those individuals responsible for security must develop three different sets of procedures for proper security configurations. And those individuals responsible for compliance must define three different work programs to audit those packages. The more energy that must go into the day-to-day administration and operations, the less time and energy is left over to concentrate on security.

Policies and standards are often confused with each another. Let us compare a policy and a standard related to the same topics: passwords and log-in IDs. A policy statement would be: "All systems must maintain a unique log-in ID." A related standard might be: "The naming convention for log-in IDs is the first four letters of a user's last name plus the last four digits of his social security number." From this standards statement, it is not very clear how this standard naming convention relates to security until it is compared to log-in IDs without a naming standard. Exhibit 3-1 lists five examples using the above standard and five examples with no standard.

With the list of non-standard IDs, an administrator, auditor, or security officer would have a difficult time understanding to whom the ID belongs and to what system it relates.

Let us continue with the comparison of policies and standards related to passwords. A password policy is: "All systems will have passwords that are

Exhibit 3-1. Five Examples Using A Standard and Five Examples with No Standard

Standard	(Last Name, SSN)	No Standard
Chad6543	Lowery_molly	(last name, first name)
Bard5431	XL334mtj	(application, user initials)
Went3332	ACCT3421	(dept, assigned number)
Drew3512	allyssaT	First Name, Last Initial
Kill1432	megan3422	First Name, SSN

changed on a periodic basis.” The related standards statement is: “All passwords will be a minimum of eight characters in length and contain both alpha and numeric characters. User passwords will be changed every 90 days. Administrator passwords will be changed every 30 days.” The policy tells us that we must establish user IDs and passwords. The standard defines exactly what those IDs and passwords should look like. A related procedure will define how passwords and user IDs are actually set up; for example, what forms are used to request user IDs, who should the form be sent to, and who needs to authorize them.

Another way of looking at standards is that they are preformulated guidance, in which the issues, considerations, and effects of doing something have already been analyzed by someone authorized to make a decision for a group. For example, take an organization with seven different operating locations in which Windows XP is a prevalent operating system throughout the organization. Now assume that there are seven different Windows XP administrators, each at a different location. It would not make sense to have each administrator come up with his or her own way of configuring and operating the system. A more efficient approach would be to identify who, within those seven administrators, has the most experience and complete set of documentation related to the configuration and operation of Windows XP. This information should be compared with industry best practices, and then a set of standards and procedures should be formulated and disseminated for use by the other six administrators.

Standards development can be achieved by the Security Team or a subset of individuals on the Security Team, augmented by both internal and external experts on the subject. In the Windows XP example, it would make sense to have several or possibly all of the administrators form a subgroup for the development of standards related to Windows XP. The Security Officer chairs the subgroup as the project manager and drives the objectives, documentation, and deliverables for the project.

Standards Organizations

There are also many groups created just to formulate standards, including:

- *ANSI*: American National Standards Institute
- *CCITT*: Consultative Committee on International Telephony and Telegraphy
- *ECMA*: European Computer Manufacturers Association
- *EDPAA*: Electronic Data Processing Auditors Association, Inc.
- *EIA*: Electronic Industries Association
- *IEEE*: Institute of Electronics and Electrical Engineers, Inc.
- *IAB*: Internet Architecture Board
- *IESG*: Internet Engineering Steering Group
- *ISO*: International Standards Organization
- *NIST*: National Institute of Standards and Technology
- *NSA*: National Security Agency
- *UL*: Underwriters Laboratory Inc.

Security standards come out of these committees as well as several other groups formed specifically to focus on information, system, and network security. Those groups include:

- *CERT*: Computer Emergency Response Team
- *CSTC*: Computer Security Technology Center
- *EDPAA*: Electronic Data Processing Auditors Association, Inc.
- *FACCI*: Florida Association of Computer Crime Investigators
- *FIRST*: Forum of Incident Response Teams
- *GSSP*: Generally Accepted System Security Principles Subcommittee
- *HERT*: Hacker Emergency Response Team
- *ICAT*: Initiatives for Computer Authentication Technology
- *ICSA*: International Computer Security Association
- *NIST*: Computer Security Division
- *NSA*: National Security Agency
- Information Assurance Technology Analysis Center
- International Information Systems Security Certification Consortium
- Laboratory for Information Security — George Mason University
- Network Security International Association
- San Diego Regional Info Watch
- SANS Institute

An example standard is Secure Electronic Transactions (SET), which allows World Wide Web software developers to incorporate the means for accepting encrypted credit card payments. Technical specifications of this standard were published in 1996. This standard was agreed upon by Visa and MasterCard to offer secure shopping over the Web. Other specifications developed for the same purpose but not accepted as a standard were the Secure Transaction Technology (STT) developed by Visa and Microsoft Corp., and Secure Electronic Payment Protocol (SEEP) developed by MasterCard and Netscape Communications Corp.

INFORMATION SECURITY ARCHITECTURE

Other organizations and associations are initiated to develop standards within certain industries. The American Bankers Association has developed the Accredited Standards Committee X9 for Financial Services. This association has been responsible for such security standards as Personal Identification Number (PIN) Management and Security (X9.8), Financial Institution Message Authentication X.9.9, Financial Institution Retail Message Authentication X9.19, Transmission of Personal Authenticating Information and Node Authentication, and Encryption of Wholesale Financial Messages X9.23.

A more recently developed organization in the banking industry is BITS (Banking Industry Technology Secretariat), a division of Bankers Roundtable. BITS focuses on technology issues affecting the U.S. banking system and is governed by a board of CEOs of the 15 largest U.S. banks, including Citibank, Chase Manhattan, Mellon Bank, First Union, Wells Fargo, and Bank of America. BITS has formed a test lab to address the security issues related to the link from the bank to the home computing environment. Security experts from major banks are drafting testing criteria to test consumer devices and software, and will also test systems to conduct financial transactions, including personal financial software, online billing, bill-paying packages, and smart cards. To a greater extreme,

BITS lab oversight group is working with the President's Commission on Critical Infrastructure Protection on ways to protect the nation's financial infrastructure from attacks by terrorist or organized criminal groups. This effort involves information sharing among banks to ward off organized attacks, including use of neural networking and other technologies to detect and predict patterns of attacks.

Working Groups for security in the healthcare industry include Computer-Based Patient Record Institute (CPRI), Healthcare Open Systems & Trials (HOST/MCC), and National Information Infrastructure Testbed-Health Care Work Group (NIIT). Accredited Standards Organizations include:²

- *ASTM E31.17: Access, Privacy, and Confidentiality:* promotion of knowledge and the development of standards addressing confidentiality, access, and security of computer-based patient records and data derived from computer-based patient records.
- *ASTM E31.12: Computer-based Patient Records.*
- *ASTM E31.20: Authentication of Health Information:* defines the process for authentication in computer-based patient record systems focusing first on clinical information but including all related healthcare information such as eligibility and purchasing authentication.
- *ANSI HISSP: Health Information Standards Planning Panel.*

Legislation related to the work of these groups includes the Health Care Security Act (H.R. 3600) and the Fair Health Information Practices Act (H.R. 4077).

Within the Internet community, there are working groups that write what are known as RFC (Request for Comment) documents, which are Internet standards-related specification documents. The documents are numbered, named, and published on the Internet for review and comment by anyone who wishes to provide input to the document. Comments are typically provided back to a point of contact who then submits the recommendations to the working group for modification to the document. There is a formal process for submission of an RFC and they are classified into status categories: proposed standard, draft standard, standard, best current practice, informational, and experimental. This process is organized and managed on behalf of the Internet community by the Internet Architecture Board (IAB) and the Internet Engineering Steering Group (IESG). An index of RFC documents can be found at <http://www.faqs.org/rfcs/rfc-index.html>, with search capabilities at <http://www.faqs.org/rfcs/>.

Two good RFC documents used to develop security policies and standards are RFC 2196 (The Site Security Handbook) and RFC 1281 (Guidelines for the Secure Operation of the Internet). RFC 2196 originated in 1991 and superseded RFC 1244 in 1997. This handbook is the product of the Site Security Policy Handbook Working Group (SSPHWG), a combined effort of the Security Area and User Services Area of the Internet Engineering Task Force (IETF).

Standards, policy references, general security information, and Web sites can be found at:

- <http://www.gartner.com>
- <http://www.infosyssec.org>
- <http://www.bitpipe.com>
- <http://www.diffuse.org/secure.html>
- <http://www.rsasecurity.com/standards/>

General security lists are available in Appendix A-6, which provides information on how to subscribe to security list servers on the Internet. These security lists include advisories, exploit scripts, security best practice information, bugs and security holes, and information on privacy, cyphers, and underground and hacker organizations.

There are many security standards to cite. The developers of standards must have an understanding of both the risks and the operating environment to begin to formulate logical, operationally feasible standards. The table of contents from the Security Standards and Procedures Manual (SS&PM) as shown in Appendix A-7 is organized into logical groupings of standards. This list provides a point at which to begin the development process. Specific security standards related to each operating system (UNIX, Windows XP, Novell Netware, VMX, etc.) and application should also be developed.

Security Procedures

Policies should be developed first to provide direction and guidance in the development of standards and procedures. Once policies are in place, standards are developed to define uniform methods of complying with policy. As stated in the beginning of this chapter, procedures are plans, processes, or operations that address the specifics of how to go about a particular action. They enable the transfer of knowledge between individuals who perform the same job, cover for each other during periods of absence, or allow for a more knowledgeable and smoother transition during permanent changes in staff. Procedures should reflect best practices that have been established or through the repetitive nature of performing a specific task, improvements that have been made to the process to provide for efficiency. Procedures are also guidance but typically answer the more detailed questions of where, when, and how.

Procedures are not typically written by committee or by the Security Team. For organizations in which procedures have not yet been documented, it is necessary to interview the individual responsible for the day-to-day operation of that procedure. By documenting current practices, deficiencies in the process can be identified and corrected to make the process more efficient.

The sample procedure in Appendix A-8 defines an anti-virus software implementation. First, let us review the related policies and standards for this topic. The security policy statement is: "Anti-virus software will be used on all firewalls, mail servers, and desktops." The related standards statement is: "Virus definitions will be updated, at a minimum, on a biweekly basis or more often as necessary to respond to newly generated viruses." The procedure tells us specifically what software is running on each platform, who is responsible for loading the definitions, how to download the virus definitions, how often the scans are loaded and executed, and what tests are performed on the software prior to loading to production machines.

It is clear that this procedure has been written for a specific operating environment and configuration. Each procedure must be defined by the administrator responsible for the execution of that procedure. By looking at the content in this procedure, several items should be noted. The procedure indicates the:

- Objective of the anti-virus program
- Person responsible for each work step
- Review date
- Review authority
- Location of related procedures, referenced test scripts, and executable files, if necessary
- The purpose and scope of each related version test

Procedures should be written to such detail that the reader can perform the functions described without having to ask for clarification about what files to access, who to call for problems, or where to find the tools necessary to perform all steps related to the procedure. More often than not, procedure documentation will not be used by the individual who performs it on a daily basis, but rather by that individual's backup during times of illness, vacation, or change in staff.

Procedures are not typically reviewed at the executive level; they are generally reviewed for completion and content by those individuals responsible for the development of the Security Standards and Procedures Manual (SS&PM). Like policies and standards, procedures should be reviewed on an annual basis to ensure that they are valid.

In the hybrid security organization, policies and standards come from the Security Team. Procedures are the responsibility of each operating system, application, network, and database owner and administrator. These procedures should be defined at the business unit.

Chapter Summary

Security policies are the foundation of the organization's ISA. Their purpose is to inform all users about the expectations of management regarding the appropriate use of information, systems, and resources throughout the enterprise. They must be disseminated throughout the organization and enforced. A general security policy should define the security objectives of the organization, the resources requiring protection, security responsibilities of key players, and resource ownership. The security policy objectives include security management, confidentiality, integrity, availability, authentication, non-repudiation, and access control. The security policy dictates the security programs that must be implemented to meet the policy objectives. These programs include risk assessment, monitoring and enforcement, awareness and training, computer emergency response, disaster recovery, and business continuity.

Standards consist of a specific set of rules, procedures, or conventions that are agreed upon for more efficient and consistent operation. Security standards ensure that individuals operate consistently to minimize risk and to make administration of systems and networks more efficient. Security standards should reflect industry best practices. Some of the more well-known security standards producing organizations include CERT, CSTC, FIRST, GSSP, HERT, ISSA, NSA, and SANS Institute. Security standards include the designation of encryption algorithms and key strengths for banking operations, operating system security configurations, and Internet-related standards documents known as RFCs (or Requests For Comment). Two good security-related RFCs include RFC 1296 (The Site Security Handbook) and RFC 1281 (Guidelines for Secure Operations of the Internet).

INFORMATION SECURITY ARCHITECTURE

Security procedures document the best way of performing a function. They also provide consistency of operations between individuals who perform the same job, and are most important when the primary administrator is unavailable and a backup must take over responsibilities. Examples of security procedures are found in Appendix A-7, the SS&PM Table of Contents. They include procedures on requesting, setting up, and deleting user accounts and system and resource access; the administration of passwords; backing up operating systems, files, and data; change control; and anti-virus maintenance, logging, and reporting.

Some policies, standards, and procedures related to security are becoming required by law, particularly in the banking and healthcare industries. Policies related to patient confidentiality or privacy of information must be directed in writing and provided to the client in these industries. Due to the constantly changing systems environment, policies, standards, and procedures must be continuously reviewed and updated to reflect the nature of the current environment.

Employees contribute to the objectives of the organization by following the policies, standards, and procedures outlined for them in the performance of their job responsibilities. Documented policies and standards are the basis for measuring compliance throughout the organization by defining a set of rules against which to test.

Getting Started

1. If an Information Security Policy is not already in place, gather several template policies from the Web sites listed previously. Selectively choose policy statements that fit best within the organization's operational environment and corporate culture.
2. Once a template policy has been developed, disseminate the policy to members of the Security Team for review. Call a meeting of the Security Team to go over each paragraph of the document.
3. Consolidate suggestions and modifications, and resubmit the revised policy for a second review by the Security Team. This iterative process should continue until few or no suggestions are being offered. Do not become discouraged at heated debates over Security Team member opinions and suggestions. The alternative is to have no one desire to actively participate in the policy's modification and development. Heated discussions are good. This process solidifies the policy content in the mind of each participant. It also attaches a sense of ownership of the policy for each of the participants. Ownership encourages a willingness and desire to enforce the policy.
4. Once a consensus of the policy has been reached, the policy should be presented to Executive Management for review and approval.

5. Approved policies should be announced and disseminated throughout the organization. They also need to be incorporated into new-hire training sessions.
6. The Security Team then needs to review the existing security standards within the organization. Begin by looking at the table of contents of existing policy and standards documents. Review the table of contents, comparing it with the SS&PM table of contents provided in Appendix A-7. Determine what standards have not been documented.
7. Interview appropriate administrators to determine if *de facto* standards were put in place and are simply not documented. Document the standards described by each of the administrators interviewed.
8. Assign tasks and timelines to each of the Security Team members to draft portions of the SS&PM.
9. Consolidate standards for Team member review and follow the same procedures described above for policy development.
10. Procedures should also be developed for each security program administered centrally. A requirement should be dictated to business unit administrators for the development of component-specific procedures. It may be appropriate to hold subgroup meetings between common component administrators to coordinate and document existing procedures.

Notes

1. Tim Clark, Big Banks Move on Net Security, *CNET News.com*, May 21, 1999.
2. *Computer Security Journal*, Vol. XI, No. 1, 1995.

Chapter 4

Security Baselines and Risk Assessments

To understand the level of risk that exists within the operating environment, periodic risk assessments need to be performed. In distributed computing, nothing remains constant. Vulnerabilities, loopholes, and backdoors are being discovered all too frequently. In large operating environments with multiple platforms and hundreds of servers, ensuring that a single security hole is fixed can be costly and time-consuming. A program for understanding and managing risk is the topic of this chapter. This chapter reviews the areas for assessment and provides sample workplans for those reviews.

When a new system is implemented, a preliminary assessment called a security baseline needs to be performed. With new systems or systems that have never been assessed, the security posture is unknown. A baseline provides a starting point to measure changes in configurations and improvements to the system. From this baseline, periodic risk assessments will provide the current state and effectiveness of controls within that system for a given period of time.

Risk assessments educate the administrators about their systems. Most administrators are concerned with day-to-day operations, making sure the system is running and is available to the users. Security is secondary to the administrator and is often viewed as a burden or an additional responsibility that adds little value. Unfortunately, the value of a secure and well-controlled system is not tangible. The value of security becomes tangible and measurable only when an incident occurs that provides a dollar value to the loss.

Assessments are a mechanism to identify the strengths and implemented controls of a system, not just the weaknesses and risks. Assessments can provide the basis for rewarding administrators that have taken security seriously. Recognition and positive feedback are a means of keeping administrators interested in the security program. Instead of being

INFORMATION SECURITY ARCHITECTURE

viewed as a burden, the security program will become interesting, challenging, and rewarding to those who are responsible for its execution.

Assessments should be combined with teaching and training sessions. The cost of teaching and training by third parties or contractors, if added to the contract during contract negotiations, can often be negotiated into the existing price. Many consultants or contractors will throw in training to ensure that they are awarded the contract. If this is the case, be sure to require as a part of the contract a training workplan and training outlines as a deliverable of the project.

INFORMATION SECURITY ASSESSMENT: A PHASED APPROACH

The first step in identifying the areas of increased risk within an organization is to perform a high-level overview. This is necessary to gain an understanding of the magnitude of the operating environment. The topics that should be covered are:

- Operating environment
- Security organization
- Security planning, administration, and management
- Information security policies, standards, and procedures
- Information security risk assessment
- Information classification and control

To obtain a high-level understanding of the operating environment, it is necessary to gather the appropriate information. The following is a list of documents that should be gathered prior to this review.

- Organization chart
- Security policies, standards, and procedures documentation
- Network diagrams
- List of applications
- List of network management tools
- List of security assessment tools
- Asset inventory
- List of databases
- Reports from previous assessments and audits

In an organization with centralized control of the security program and decentralized administration of security, it is necessary to understand the mechanisms in place to ensure that the security program is effective from the central organization down to the business unit and administrator level. Section I of the Information Security Assessment Workplan provides an overview concentrating on the management of specific programs developed as a part of the ISA and the allocation of security responsibilities. Once this has been identified and validated, the assessment should focus

on more operational levels of security. Section II of the Information Security Assessment Workplan reviews:

- Security monitoring
- Computer virus controls
- Microcomputer security
- Compliance with legal and regulatory requirements

The next two sections concentrate on general computer controls that include computer operations in Section III and a review of application access in Section IV. Computer operations personnel are responsible for the daily execution of programs, the backup of systems, data and programs, and resolution of any issues that arise from errors or improper execution of the program. Section III, Computer Operations, includes:

- Physical and environmental security
- Computer systems management
- Backup and recovery
- Problem management

Section IV reviews those areas related to applications: access controls, application development and implementation, and change management.

Once these areas have been reviewed, the security assessments need to become more granular, moving to the business unit and to the systems and applications supported by that business unit. This portion of the assessment will identify specific vulnerabilities within each system. More detailed security assessment workplans are discussed later in this chapter for telecommunications and networks.

HIGH-LEVEL SECURITY ASSESSMENT (SECTION I)

Assessing the Organization of the Security Function

An assessment of the security organization should document the number of individuals performing security functions, including full-time security positions as well as individuals that dedicate only a portion of their time to security. This assessment also includes an understanding of to whom these positions report. Segregation of responsibility is essential. For example, the full-time security positions may report directly to the CIO but should not be under the direct management of the development and operations group. The security function should maintain independence from the system user departments. It is difficult to be objective and effective in enforcing security when one works directly with or for those same individuals. In this same vein, an independent committee or counsel should be reviewing the planning, operations, and output of the Information Security Group.

INFORMATION SECURITY ARCHITECTURE

The security mission and charter should be documented and describe how the mission ties to each of the business units. It should also describe how the security organization interfaces with and influences system development and software acquisition related to security controls and considerations.

Assessing the Security Plan

The Information Security Plan should be documented and describe support for the goals and objectives of the Strategic Information Technology Plan. In assessing the Plan, determine who is responsible for its development, review, approval, and implementation. Responsibility for, as well as target completion dates, should be defined for each project, initiative, or strategy defined in the Plan.

Assessing Security Policies, Standards, and Procedures

Determine how policies, standards, and procedures are developed, reviewed, approved, and modified and who is responsible for each step of this process. The policies and standards should cover security management and administration, information access control, user identification and authentication, data ownership, security monitoring, compliance testing, software licensing, physical security, report storage, distribution, and destruction procedures, and should include penalties and measures for noncompliance. Determine if there is a mechanism for enforcing policies and measuring compliance.

Assessing Risk-Related Programs

Programs for risk assessment include classification methodologies, business impact analysis (BIA), incident and emergency reporting and response, disaster recovery planning (DRP), business continuity planning (BCP), and incident monitoring, investigation, and remediation. Determine who is responsible for each of these programs, if the program has been documented, and if they are being implemented and reviewed periodically.

Appendix B-1 is an Information Security Assessment Workplan that provides a high-level overview of the security environment and addresses questions related to security organization, planning, administration, and management. This questionnaire is not all-encompassing. It is to be used to begin the process of understanding and documenting the current state of the operating environment. More detailed questions describing the defined processes should be asked as the interview or assessment process continues.

Exhibit 4-1 displays a document checklist that should be provided to the business unit under assessment. The checklist can be used to follow up on documents not initially provided and as input to a workplan that details the programs and documents that need to be developed.

Exhibit 4-1. Assessment Document Checklist

- Organization chart
 - IT strategic plan
 - Information security plan
 - Security charter or mission statement
 - Security policies, standards, and procedures
 - Policy acknowledgment forms
 - Confidentiality agreements/statements
 - Network diagrams
 - Maintenance and service contracts with third-party service providers
 - Application inventory
 - Hardware asset inventory
 - Network management tools inventory
 - Security assessment tools inventory
 - Database inventory
 - Classification methodology
 - Audit programs
 - Compliance checklists
 - Security assessment reports
 - Resource ownership matrix
-

Completion of the Information Security Assessment Workplan and obtaining and reviewing the documents listed in the Assessment Document Checklist will provide a good understanding of the programs in place to administer the Security Program and the current security posture of the organization. Once an understanding of the operating environment and security program administration is obtained, it is necessary to assess at the component level.

SECURITY OPERATIONS (SECTION II)

In Section II of the Information Security Assessment Workplan, there is a shift in focus from program management to operational security programs. These programs include the operational implementation of security throughout the organization.

Security Monitoring

Security monitoring includes those processes in place to identify and investigate suspected access violations and attempted system intrusions. This includes audit trails of security-related events. Several examples of this type of monitoring include:

INFORMATION SECURITY ARCHITECTURE

- Daily review of remote access log-ins to identify failed access attempts
- Review of system access logs for access to systems during non-work hours
- Review of traffic on external gateways
- Review of access to application system utilities and privileged user activities
- Review of access to sensitive files or data

Software exists that will automatically monitor system logs for specified events and alert administrators when those events are triggered, indicating a potential intrusion attempt.

Procedures are necessary for reporting and responding to suspected violations. These procedures need to be communicated throughout the organization so that all users can report suspected activity and security personnel can respond efficiently and effectively to that activity. Once an incident has been validated and escalated, procedures must exist to appropriately report the incident to management as well as define remediation efforts to ensure that the exploited vulnerability is eliminated so the situation does not recur.

Computer Virus Controls

Effective computer virus controls are an absolute necessity. There are so many ways a virus can now enter an organization's operating environment; e-mail attachments, Internet ftp downloads, and floppy disks inserted into workstations are but a few. A very effective computer virus program was described in the Anti-Virus Upload Procedure example in Exhibit 3-3 of Chapter 3. This three-tiered architecture included anti-virus scans at the workstation, mail servers, and firewalls. To be effective, however, current virus definition files must be in place. Depending on the size of the organization, the effort to ensure current virus definition software is uploaded to each workstation on a biweekly basis can be an administrative nightmare.

For anti-virus security assessments, it is necessary to ensure that procedures exist to:

- Download current definitions from the appropriate sources on a timely basis
- Test virus software before distribution
- Distribute and upload current definitions to all platforms (servers, mail servers, firewalls, and workstations)
- Validate that distribution of software and definition files is effective
- Ensure compliance with all anti-virus software procedures
- Assess the communications mechanism between administrators and users on potential viruses and the reporting of suspected viruses

Microcomputer Security

Traditional management focus for security has been on minicomputer and mainframe environments. Technology has enabled many functions reserved for these platforms, such as financial and management reporting, to migrate down to the PC. For this reason, security concerns in the mini- and mainframe environments are similar to those of the microcomputer.

Software licensing has become a major issue with organizations being caught and fined in the hundreds of thousands dollar range for copyright infringement. Ensuring that copyright infringement does not occur includes:

- Monitoring licenses registered versus licenses used
- Inventorying PC software
- Defining and distributing approved software lists
- Developing software usage policies

The second area of concern related to PCs is physical security. Both desktop and laptop computers are difficult to secure because of their portability as well as the use of desktops and laptops in common office areas. A review of physical security should include physical security of platforms, disks, work rooms, offices, and building security. PCs should also require passwords upon log-in and application and network timeouts for inactivity. Critical business data that is transferred from the mainframe, mini, or other PCs should be protected at the same level of security as the original environment.

Backup and contingency plans apply to PCs as well as all other systems. PC programs and data files must be backed up regularly. Network servers should be allocated to store critical application data and programs that are processed in a client/server environment, eliminating the use of the PC's hard drive for such activity. PC applications that have significant importance to business operations need to be identified and protected from unauthorized access, as well as for contingency planning. Contingency planning includes the replacement of PCs for losses due to fire, flood, or other disasters.

An assessment of microcomputer security should include procedures to:

- Prevent the use of unauthorized software
- Provide training to all PC users
- Ensure physical and logical security of PCs used for critical business operations
- Ensure PC software development adherence to approved software development and maintenance methodologies
- Provide adequate documentation of PC applications to users
- Ensure the integrity of all data, applications, and information processed on the PC
- Provide for backup and contingency plans for PC hardware, software, and peripherals

COMPLIANCE WITH LEGAL AND REGULATORY REQUIREMENTS

Many industries are required to adhere to privacy regulations and legal requirements related to protecting the information of customers. The financial and healthcare industries are both strongly regulated. Organizations within regulated industries typically have designated personnel or departments assigned to monitor compliance to regulations. A security review of these areas should be conducted to ensure:

- Guidelines on the retention, storage, and handling of regulated information
- Appropriate protection of classified data
- Compliance with regulatory requirements
- Compliance with legislation protecting information

COMPUTER OPERATIONS (SECTION III)

Computer operations personnel are responsible for the physical security of the central processing facility, ensuring the proper execution of programs, maintaining system and critical data backups, responding to and resolving execution errors, and providing assistance in the recovery of systems, programs, and information.

Physical and Environmental Security

The physical security of critical applications is essential to prevent unauthorized access to computing facilities and to provide proactive measures in the chance that a natural disaster might occur. A review of physical controls includes locks, guards, and documentation of access. In an assessment, check for the use of:

- Cypher or key pad locks
- Fencing
- Guards
- Monitoring devices
- Maintaining authorized personnel access lists
- Limiting access to only essential operations personnel
- Maintaining sign-in logs
- Badges

It is important that computing facilities be located away from potential environmental hazards. This includes chemical plants, fuel sites, significant water sources, airport approach patterns, and waste facilities. Environmental controls should be in place to protect against fire, flood, and other potential disasters. Environmental controls include:

- Backup power (uninterruptible power systems [UPS])
- Air conditioning
- Fire suppression devices (fire extinguishers, halon, other)
- Fire detection devices (sensors)

- Heat detection devices
- Business continuity plans (BCPs)
- Alternative processing facilities
- Disaster recovery plans (DRPs)
- System and data backups

Backup and Recovery

Backups are a crucial responsibility for any organization relying on systems for critical business processes. Backups must be performed so that system, program, or information loss or damage can be efficiently restored. The frequency of backups will determine how much information will potentially be lost between backups. Backups should be stored out of the processing facility so that any disaster at the facility will not compromise the backups as well. Removing backups from the facility creates a requirement for ensuring that those critical backups are not subject to unauthorized access by vendors or outside personnel. Review who, when, and how third-party vendors obtain, transport, and store those critical business system backup tapes. All too frequently, these tapes are placed outside a locked facility in an uncontrolled area so that the vendor can drive by and quickly pick up the tapes with ease. Ensure that accountability is established for the transfer, transport, and storage of this information. It is not uncommon to request a review of a third-party vendor's procedures to ensure that they are as conscientious about security and meet the minimum security requirements set by the organization.

Internal tape management as well as by third-party vendors is also very important. If tapes are not properly marked, it will very difficult to determine which tapes are necessary to perform recovery operations. Labeling, rotation, and reuse of tapes is important when the use of backups becomes necessary.

As a part of physical security, backup processing locations are important. Many vendors contract to provide alternative processing locations in case of a disaster. Remember that a localized disaster can cause a demand on the vendor performing the recovery because that vendor may have other clients in the area where a disaster occurs. It is necessary to understand under what disaster scenarios the vendor will be used. Ensure that vendors sign nondisclosure agreements; remember that they have access to proprietary and critical business systems and information.

Recovery plans should be tested annually. This includes loading critical software at the backup site and preparing for alternate site processing. Testing of recovery plans provides the assurance that operations move as planned to minimize damage when an incident occurs. Recovery plans should be based on a business impact analysis (BIA) that identifies the areas of greatest risk of financial and operational losses to the organization. As system, applications, and processing methodologies change,

reevaluation of the BIA is necessary to ensure that the recovery and continuity plans focus on those areas of greatest risk.

Computer Systems Management

Computer systems management includes the daily execution and maintenance of systems, applications, and information. Operational procedures must be clearly defined, updated frequently, and documented to ensure an efficient transfer of responsibilities between shift operators and backup personnel. The computer operations department should maintain a log that details the execution, completion, and issues identified during the shift. This log should be reviewed by management and jointly reviewed by both the outgoing shift personnel and incoming shift personnel so that continuity and efficiency are maintained.

Computer operations personnel should be restricted from read, write, and delete access of computer programs. Their primary focus is the execution of programs. Often, operations management deems it necessary for operations personnel to have write access so that errors and abends in program runs can be corrected immediately by the shift operator. When this is necessary, mitigating controls must be adhered to. These include a review by the supervisor of program change logs, documentation of changes, validation of changes, and follow-up testing. Control is better maintained when operations personnel are given access as necessary to make changes, and then access is removed after the issues have been resolved.

Computer operations personnel should also be restricted from accessing source code, limited to only the executable version of the program, and should not have access to development and test environments. Maintaining separate development, test, and production environments minimizes the risk of executing the wrong version of software.

Computer operations personnel should be involved in the change control process and status meetings to ensure that the impact of changes is known.

Problem Management

A problem management process needs to be in place to report, track, and resolve problems incurred in computer operations, as well as in dealing with security-related issues. Problem management also includes the measurement of the number and types of problems against the service levels expected. Problem management is not just the resolution of problems, but also the:

- Reduction of failures to an acceptable level
- Prevention of the reoccurrence of problems
- Reduction of the impact on service

Problem management is an integrated function and should not be associated only with computer operations, although this is the area it has been placed within this chapter and within the Information Security Assessment Workplan. The problem management control process includes system planning, programming, and network control. Problems should be categorized according to the level of severity and impact. This provides efficiency in directing the issue to the appropriate individuals skilled at dealing with the problem.

For organizations that support a Help Desk, the Help Desk's primary goal is first-level problem resolution: attempting to recognize and localize the problem to a specific category. Those problems that cannot be quickly resolved at the first level of support are passed to the group responsible for the identified and localized problem. Examples are server hardware, networks, application software, or the PC itself. The problem is passed to a more technically qualified individual whose primary responsibility is related to the day-to-day maintenance of the specific piece of hardware, software, or system.

Problem resolution should include:

- Providing a centralized point of contact for problems
- Logging problem calls
- Resolution of problems quickly and efficiently
- Transferring unresolved problems to more technically qualified personnel
- Tracking and managing difficult problems
- Identifying recurring problems, analyzing root causes, and providing permanent resolution
- Improving communication and training to end users
- Reporting the status of issues to management, users, and departments impacted
- Evaluating vendor performance and service-level contracts based on the level of support provided in resolving issues

Sections I through III of the Information Security Assessment Workplan provide an overview of the security posture of the organization. After completing these sections, areas of risk and needed improvement related to the security program should have surfaced. The remainder of this chapter provides a more detailed review of the layers of the operating environment: applications, databases, networks, and operating systems. A separate workplan is available within the appendices for each of these topics.

APPLICATION CONTROLS ASSESSMENTS

Security control assessments related to applications primarily focus on the appropriate access of users, administrators, and programmers to application data and functionality, system files, program modules, and hardware

resources. Access controls are designed to ensure appropriate authorization of resources. A review of application controls should also consider authentication, availability, confidentiality, and integrity. Controls related to these areas are discussed in this section and include segregation of duties, the use of audit trails, authentication methods, and database issues. Several areas that are integral to the security of an application are computer operations, application development and implementation, and change management. These areas fall under general computer controls that support the operation of applications and should be assessed in conjunction with an application security assessment. Computer operations was also discussed in Section III of the Information Security Assessment Workplan. It is included again under applications, but focuses primarily on application-specific computer operations. Application development, implementation, and change management is included in this section of the chapter. A separate workplan at Appendix B-2, Application Controls Assessments, details the guidance provided in this chapter.

Access Controls

The assignment of data owners is extremely important in establishing proper authorization. Data owners are the individuals who ensure appropriate authorization is granted for access to the owned information. Data owners approve access based on job requirements and functionality. For this reason, role-based access is the most logical method for setting up access to an application. It is also the most efficient method and simplifies the access management process.

A process should be in place to make a formal and documented request for user access. This request needs to be approved by the appropriate individual who is knowledgeable about the functionality of the application as well as the job that the user will be performing. This documented request should be maintained and any changes to access should be annotated on the request. Request forms should be reviewed and compared to actual access control lists (ACLs) on a quarterly or semi-annual basis. This control will identify any errors that may have been made in setting up or modifying the user's account.

Role-based access is determined by an employee's job function — not by who the employee is as a person. Based on the employee's role in the organization, he or she is given access to certain functions or menus within the application. If an individual leaves the company, the individual taking over that particular job function will automatically be given the same level or type of access. The role or access template can be copied and assigned to the new user's ID. This reduces the time it takes to set up each individual user and minimizes the introduction of errors. An employee who performs several functions or roles will be provided with levels of access for the multiple job functions they perform. Data owners are responsible for reviewing user

access rights on a regular basis to ensure that the approved access remains appropriate.

To perform an assessment, generate an access control list (ACL) report on all users registered to the system. The first check performed should be to validate whether the owner of the ID is still on payroll. Many organizations have coded automatic routines that compare a user ID list to a list of current employees and flags those employees who have terminated their employment with the company or moved to other departments. This is the most efficient and timely way of ensuring that application access is in line with moves, adds, or changes of employees.

The next check should be to evaluate each user's access rights and compare them to the user's job description, ensuring the appropriate segregation of duties. This check is normally performed by the data or application owner and is often delegated to the department's security liaison. A common audit issue or security finding is that access right assignments are left up to the technical application or operating system administrator. This can often be an individual whose background is in computer technology and is not trained in the functional business area supported by the application. This individual may not understand the specific segregation of duty requirements necessary to ensure security for the business unit. This is why it is very important that security roles within the company are formally defined and that data owners or security liaisons work with technical administrators to establish the correct access privileges.

Application access is typically controlled by menus that restrict user access to certain functionalities of the application. Some legacy systems do not provide menu and module access controls. In these cases, if a user has access to the application, then he or she may have access to the entire system. Sometimes, access control software can be overlaid on the application software. Examples of access control software include ACF2, RACF, Top Secret and control mechanisms within CICS. If none is available, compensating controls need to be identified to ensure that abuse of application access will be identified by those compensating controls.

Separation (or Segregation) of Duties

Separation of duties ensures that no single employee has control of a transaction from beginning to end. For example, anyone allowed to create or certify a transaction should not be able to also execute it. Separation of duties guards against manipulating a transaction for personal gain. The most common example for segregation of duties is to ensure that an accounts payable clerk does not have the ability to change or maintain vendor lists. Many fraudulent checks are produced each year by accounts payable personnel who make up phony vendors and then pay those vendors with small dollar checks that do not need management approval.

Another example of functions that should be separated is typically accounts payable and accounts receivable, for very similar reasons — having the ability to submit false receivable documents and also the ability to pay them. Individuals in computer operations should have the ability to execute programs but not have write capabilities to these files. There must also be a separation of duties between system programmers and system operators. This is discussed later in the chapter regarding the assessment of program change management.

Audit Trails

Audit logs are a record of system activities that provide the capability to reconstruct the sequence of events related to a transaction. Audit logs can be used to determine errors in system processing as well as misuse of the system. In an assessment, the system and application should be reviewed to understand the auditing capabilities and to assess if the audit functions are turned on and are reviewed. A mechanism should tie a user's ID to the transactions that the user has performed or attempted and to changes that user has made to the system. Access to application system utilities and privileged user activities should be monitored daily. Violation reports that log security-related events, such as unsuccessful access attempts, should also be monitored daily.

Application system utilities are sensitive because they bypass application access controls and allow direct access to production code and data. These utilities should be protected by passwords and should not be accessible from the application. It is necessary to test that users cannot break out of the menu and obtain the system prompt. Breaking out to the command line is generally operating system specific. Access to system utilities should be limited to a minimum number of essential and trusted persons. Unnecessary application and system utilities should be removed.

Authentication

Application authentication must also be assessed. Authentication as it relates to application access is defined as the reconciliation of evidence of user identity. There are three ways a user can identify himself to an application or system: presenting something that only the user knows (e.g., password), presenting something that only the user has (e.g., secure token or card reader), or presenting something that the user is (e.g., fingerprint, retinal scan, or voice verification). An example of each follows:

The use of a password for authenticating a user is the most common method and is known as simple authentication. Passwords are something that a user knows. It is the least secure method of authentication because a password can be stolen and used by someone else. The fact that the password has been stolen may go unknown to the user.

Something the user has, such as a secure token, can only be used by the person in possession of that token. An example of secure tokens are credit card-size hardware that produce a one-time password only valid and usable for a small window of time, such as one minute. The user must be in possession of the credit card-like device and present the number generated by the device to an authentication server when prompted. If the token generator is stolen, it is more likely that the owner of the token generator would know that it has been stolen because the owner is no longer in possession of it. Possession of a piece of evidence that confirms a user's identity provides a stronger validation of that user's identity.

The third method of authentication is to provide something that the user is. Passwords and tokens can be stolen, but there is no known method of stealing a person's fingerprint or retina. Fingerprints and retinas are unique to every person and they represent who the person is. Using this method for authentication provides absolute assurance that the person logging on to the system is who he says he is. This is called strong authentication.

Using combinations of methods increases the strength of the authentication. For example, if a user must provide two passwords, the level of assurance increases. Applications that are highly sensitive and require stronger validation of the identity of the individual accessing the system can implement two-factor authentication. In two-factor authentication, there are two pieces of evidence to validate the identity of the user. Two-factor authentication will use a combination of two of the authentication mechanisms. For example:

something you know + something you have = two-factor authentication
something you know + something you are = two-factor authentication
something you have + something you are = two-factor authentication
something you know + something you know = two-factor authentication
something you have + something you have = two-factor authentication
something you are + something you are = two-factor authentication

The use of password protection for applications is very important. Password parameters should be the same if not very similar to the security standards for network, screen saver, voicemail, e-mail, and other systems that require passwords. Password parameters include:

- Application lockout after so many failed attempts to log on (e.g., three failed attempts)
- Minimum password length (e.g., eight characters)
- Specified password structure (e.g., a combination of alpha and numeric characters or the use of passphrases¹)
- Password change frequency (e.g., every 30 days)

INFORMATION SECURITY ARCHITECTURE

- Passwords must be unique
- Passwords must be encrypted
- Maintain encrypted password files
- Maintain password history (e.g., last ten passwords cannot be reused)
- Establish password cycle time (e.g., minimum of five days before the password can be changed²)
- Non-displayed fields
- Validation of password before passwords can be changed
- Limitations on sharing passwords

Application Development and Implementation

A formal program for application development and implementation is necessary to ensure that appropriate controls are built into the application to provide authentication, authorization, and integrity. The application development and implementation program should ensure:

- Appropriate access to source libraries
- The ability to audit access to source libraries
- Integrity checks for the input of data to detect out-of-range values, invalid characters in data fields, incomplete data, upper and lower data volume limits, two character data ranges, and inconsistent control data
- Session or batch controls to reconcile file balances after transaction updates
- Balance controls to validate opening balances with previously closed balances, including run-to-run totals, file update totals, program-to-program totals, and hash totals on records and files
- Management authorization for the initiation of application acquisition, development, and maintenance
- Change requests documents that record the reason for the amendment, date of amendment, and appropriate approvals
- Separate test and production environments
- Documented acceptance criteria for test plans
- New programs and program changes are formally approved during appropriate phases of the development process and prior to implementation
- Formal sign-off and acceptance procedures
- Cut-over procedures to move applications from the test to the production environment
- Programmers are prevented from updating production programs
- Programmers are restricted from adding programs to the production libraries
- Segregation of duties in programming and execution of programs
- System documentation and user documentation is updated to reflect all program and operations changes

- Emergency maintenance and temporary fixes to application and system software are covered by the same procedures applied to normal maintenance
- Backup versions of software are maintained prior to making any changes to the code

Change Management

Change management refers to changes in program code, operating system configurations, or network architectures. The change management process is designed to record, schedule, approve, and communicate all processing changes throughout the organization. Change management can encompass changing a single setting on a network router, or it can entail the development of an entire application. The main objective of a formal program is to adequately communicate the change to all individuals who may be impacted by it.

An effective change management program uses an application or tool to register changes. This tool should record the change requestor's name, details of the request, business justification, approvers, estimated time to perform or implement the change, individuals responsible for modifications, individuals affected by the change, testing requirements, requestor's approval on tests, management approval, and a scheduled date of change. Check to make sure that:

- The library control systems ensure that all changes to production programs are implemented by library control administrators — and not the programmers who coded the program
- Only the applications programmers involved in the changes have access to application programs under development
- Only systems programmers have access to system programs under development
- Only library administrators have write access to system and application libraries
- Access to live data is only through programs that are in the application libraries

Change management meetings are regularly scheduled events, usually weekly or biweekly, that allow the communication of changes throughout the organization. Documentation of change management meetings should exist and be reviewed. Appropriate management approval of changes should also be available for review.

Database Security

Data used by an application is usually stored in a database. The type of database determines how that data is organized. A security review of the

database will depend on what type of database the information is in; data can be stored in a relational database, an object-oriented database, or a data warehouse. Security assessments related to the database should be performed by an individual who is knowledgeable about the specific database product and version. This section briefly touches on security issues related to more traditional databases.

Weaknesses exist in every database. In a relational database, information is stored so that a mathematical calculation can be performed on the related data. The method for accessing that information is known as sequential query language or SQL. Access is controlled through discretionary access controls (DACs) or mandatory access controls (MACs). An individual who creates a relation (correlation between several pieces of information) is the owner of that relation and can grant other users access to it. With DACs, access must be granted before a user can gain access to a view. MACs secure information by assigning classification levels or labels to data. MACs are generally more secure than DACs but require greater management and negatively impact performance.

Older versions of SQL give every user who has database access the ability to create relations. This is a powerful tool that can be exploited to gain access to information not authorized for use by every user. Another security weakness with DACs is that a user can copy a relation owned by someone else. The user performing the copy becomes the owner of the “copy of the relation,” thereby gaining access to it and essentially the original view and gaining the ability to grant access to other users. DAC in SQL does not facilitate the management of access rights. To perform a function, the user needs to be granted explicit privileges to accomplish all required tasks related to the function. Essentially, because a user needs to perform a task, that user is granted access to all the information necessary to perform that task. Granting explicit privileges gives the user a lot of access, sometimes to excess in order to perform that task. The other issue related to database access is inference. From viewing authorized information, a user is able to deduce what the unauthorized information looks like.

For these reasons, database reviews are difficult and need to be performed by someone who is knowledgeable about the database product, product version, and vulnerabilities related to the product. The reviewer should also be knowledgeable about the business unit supported by the database, the database users, and about the user functions. A common check in reviewing databases and file access is to identify all world-writeable files and validate that world-writeable access is actually necessary.

Chapter 1, Information Security Architecture, discussed the levels (or layers) of access control. Exhibit 1-1 diagrams the layered access controls. The network is the outside layer to the operating environment.

Vulnerabilities that exist in the network can be exploited to allow unauthorized individuals access to the inner components of the operating environment: the applications, databases, and the platform operating systems themselves. For this reason, an assessment of the outer layer, the networks, is essential.

Network Assessments

Networks create exposures for the internal processing environment. In evaluating the network, there are four key areas to consider: remote access, intranets, extranets, and the Internet. These connectivity types will use a variety of physical and logical configurations, to include:

- Local area networks (LANs)
- Metropolitan area networks (MANs)
- Wide area networks (WANs)
- Gateways separating the corporate WAN and/or lines of business
- Internet gateways
- Virtual private networks (VPNs)
- Value-added networks (VANs)

A Network Security Assessment Workplan is available at Appendix B-3. This workplan will assist in performing the necessary steps to understand the security posture of the networking environment.

In reviewing the network, it will first be necessary to obtain an understanding of the network architecture, network management, new technology assessment and deployment, and outage and threat response capabilities. This should be accomplished with the intent to gain sufficient understanding of the network and business environment to identify technical and business risks, and to evaluate the controls implemented for each of the connectivity types that will be reviewed. In networked environments, business functions share a communications architecture. Within this architecture, security controls and management functions should be defined and include monitoring and response capabilities. An understanding of the network can be obtained by reviewing relevant documentation and conducting the necessary interviews to understand the overall network architecture, the primary business functions that use network services, management's expectations relative to network security, and how responsibility for managing network security is assigned. The worksteps are as follows.

1. Obtain an understanding of the network architecture:
 - a. Review network diagrams and documentation
 - b. Interview data network administrators
 - c. Interview voice network administrators
 - d. Interview network device administrators

INFORMATION SECURITY ARCHITECTURE

- e. Review standards relating to networked systems
- f. Review planned migration to new technologies
- g. Review network software inventory
- h. Review network hardware inventory
- i. Identify business functions utilizing the network
2. Obtain an understanding of network management:
 - a. Identify network management tools and other utility software used in managing the network
 - b. Identify how the network management tools are utilized
 - c. Identify the devices managed through network
 - d. Identify plans or changes to network managers
3. Obtain an understanding of network security administration:
 - a. Identify policies, procedures, standards, and guidelines for network security administration
 - b. Identify responsibilities for network security administration
 - c. Identify monitoring capabilities and reports used in network security administration
4. Obtain an understanding of new technology assessments and deployment:
 - a. Identify responsibilities for change control
 - b. Identify audit/security participation in new technology plans
 - c. Identify documentation of risks in new technologies
 - d. Identify general control strategy used in introduction of new technologies
 - e. Identify testing/acceptance methods used for new technologies
 - f. Identify review process for approval of new technology plans
5. Obtain an understanding of outage/threat response capabilities:
 - a. Identify tools and approaches to reducing risks
 - b. Identify responsibility for emergency response
 - c. Identify tools/strategies for responding to emergency conditions
 - d. Identify threat incidents and priorities

Emergency Response

It is necessary to ensure that bugs, security holes, and vulnerabilities are disseminated to the appropriate individuals and that those individuals are addressing the problem. This is done through an Emergency Response Program. Emergency response does not just entail a defensive response to a breach in security. Emergency response should include proactive measures that notify all appropriate administrators of a potential loophole or concern. Emergency response also needs to include follow-up efforts to ensure that alerts, advisories, and fixes are applied in a timely manner.

With the understanding gained during the first part of the review, an assessment of security controls for each of the connectivity types should be performed. For each connectivity type, and for variations within each

type, it is necessary to identify the logical path used, devices providing security functions along the logical path, and the security controls that are available or used. The path analysis should include an identification of points of access authentication, authorization, administration, as well as monitoring and reporting.

Remote Access

Remote access is becoming a critical network function. Workers and others that need access to networked systems are more frequently accessing these resources from remote sites. Due to the sensitive nature of network access and the threat of network hacking, security measures need to be consistent, effective, and manageable. Because no control can be totally effective, a means of detecting unauthorized activities and responding to such activities needs to be provided.

In addition to traditional users, dial access is often used for remote system management and diagnostics, system development activities by consultants, and access by business associates. It is necessary to identify each access type, including access to networked devices such as routers, system maintenance ports, and access servers, and to identify the controls for each path as well as points of administration, audit and reporting mechanisms, and authorization controls. For each of the dial-in connections, the following activities will be performed.

1. Evaluate external connections and dial access:
 - a. Identify external network service providers
 - b. Identify external network users (customers, business partners, employees, service providers)
 - c. Identify access methods
 - d. Identify frequency of access
 - e. Identify nature of access
 - f. Identify services used for access
 - g. Identify time-of-day access required
 - h. Identify services used when access granted
2. Evaluate network security features:
 - a. Identify points of control for each access path
 - b. Identify points of control for each service accessed
 - c. Identify points of external control
 - d. Identify nature of control points (intended for authentication, monitoring, etc.)
 - e. Identify level of functionality for each control point
 - f. Identify responsibility for each control point
3. Develop access path schematic:
 - a. Document access paths and control points
 - b. Report observations and recommendations

Gateways Separating the Corporate WAN and Lines of Business

In many enterprises, peer-to-peer network connections are being provided between business partners and associates. Connections between each of the lines of business can potentially represent a security challenge. Effective security controls, including detection controls, need to be implemented on both sides of the network connection to help ensure the security of networked environments.

During this connectivity assessment, review controls implemented to restrict access across networks, how these controls are maintained, responsibility for maintaining the gateway, the effectiveness of the gateway implementation, and threats that could be considered to bypass gateway controls. The following activities should be performed during this connectivity assessment.

1. Identify gateway controls:
 - a. Identify authorization processes and controls
 - b. Identify authentication process and controls
 - c. Identify gateway monitoring and reporting controls
 - d. Identify incident response capabilities and responsibilities
2. Identify gateway maintenance procedures:
 - a. Identify responsibility for managing gateway
 - b. Identify management tools and software used
 - c. Identify accountability controls for gateway maintenance
 - d. Identify monitoring and reporting controls
3. Identify threats to gateway implementation:
 - a. Identify potential technical and procedural threats to gateway integrity
 - b. Selectively test threats
 - c. Identify alternate access paths to gateway or across networks
 - d. Selectively test alternate access paths
 - e. Evaluate degree of risk for each threat and potential harm to the organization
 - f. Document approved and alternate paths and controls
4. Assess effectiveness of gateway controls:
 - a. Determine degree of risk from unauthorized access, monitoring, or modification of data
 - b. Determine potential liability to organization
 - c. Construct risk matrix
5. Develop access path schematic:
 - a. Document access paths and control points
 - b. Report observations and recommendations

Current and Future Internet Connections

The Internet is increasing in importance to business users not only as a source of information, but as a means of extending corporate network

resources and for providing ready network access to customers, service providers, and business associates. Because the Internet is an open environment and unregulated, the risk to an enterprise may be significant, in that information confidentiality can be compromised or that the integrity of the corporate network can be compromised.

During this section of the assessment, evaluate both current and anticipated uses of the Internet and the security controls in place. The Internet access path should be documented and controls along this path identified and assessed. The Internet connectivity assessment should begin with an understanding of the organization's use of the network in terms of who will be using it and the functions required. The security and control mechanisms should be reviewed in contrast to existing security and control policies to ensure that the safeguards implemented effectively implement these policies.

The following activities are necessary as a part of the Internet connectivity assessment:

1. Evaluate Internet controls:
 - a. Identify Internet access points
 - b. Identify Internet user characteristics
 - c. Identify nature of Internet access
 - d. Identify control implemented
 - e. Evaluate consistency and effectiveness of control strategy
 - f. Evaluate control strategy in light of future needs and requirements
2. Develop access path schematic:
 - a. Document access paths and control points
 - b. Report observations and recommendations

Electronic Mail and the Virtual Office

Within a complex network structure supporting diverse business functions, the level of security required across the network can vary considerably. In some instances, the risk to an enterprise can justify additional security controls across the entire network architecture. In other cases, controls such as segmentation of the network can be justified.

Connectivity must be viewed from a business perspective. Information collected relative to the sensitivity of information, or the need to maintain data integrity, should be evaluated in terms of the network resources that are used by business functions. From this analysis the merits and costs of providing additional security across the network can be evaluated, providing security for specific business functions, or restricting access to sensitive nodes. Activities to be completed during this connectivity assessment include the following.

INFORMATION SECURITY ARCHITECTURE

1. Identify special security requirements:
 - a. Identify business needs for enhanced integrity controls
 - b. Identify business needs for enhanced security controls
 - c. Evaluate risk to enterprise
2. Identify network resources used:
 - a. Identify network resources used by business functions having highest risk
 - b. Identify paths used by business functions having highest risk
 - c. Document access path
3. Identify controls available to support security and confidentiality requirements:
 - a. Identify controls for each access path to support added security requirements
 - b. Evaluate effectiveness of controls to meet requirements
4. Identify other means available to support security requirements:
 - a. Identify available security tools and strategies to satisfy security requirements
 - b. Evaluate the benefit/cost of providing additional security controls
5. Identify security products and services:
 - a. Identify access authentication products and single sign-on vendors
 - b. Identify encryption products
 - c. Identify single-use password mechanisms
 - d. Identify additional security products and services
6. Document analysis results:
 - a. Document security requirements
 - b. Document path analysis
 - c. Document evaluation of security products and strategies
 - d. Report observations and recommendations

Placement of WAN Resources at Client Sites

As the need to extend the network to business associates increases, opportunities for allowing others to become a node on the organization's network or to become a node on a foreign network also increase. With each connection, the risk of unauthorized access can increase. Security vulnerabilities at the external network, or within a network where they are connected, can result in a compromise of the organization's network.

During this connectivity assessment, evaluate the risk that the organization's network can be compromised as a result of a connection to an external network. Review security measures that are available to provide protection such as firewalls and the requirements that will have to be made from a policy standpoint before such connections should be considered. In many cases, such connections should be made only after each party understands its mutual liability and has agreed to certain consistent security measures, including the right to audit the other network. This connectivity assessment should include the following.

1. Identify risk associated with peer connections:
 - a. Identify business risk associated with external connections
 - b. Identify business functions with greatest risk
 - c. Identify potential liability for unauthorized access to network
 - d. Identify potential liability for unauthorized activities on network
2. Identify controls available:
 - a. Identify existing network controls and applicability to peer connections
 - b. Identify other security measures and controls and their applicability
 - c. Evaluate control measures
3. Develop connectivity requirements:
 - a. Document procedural requirements for connectivity
 - b. Document administrative requirements for connectivity
 - c. Develop connectivity strategy
 - d. Report observations and recommendations

Examine physical security in terms of the protection of network devices and cable. In this assessment include the following.

1. Physical risk identification:
 - a. Identify physical network paths
 - b. Review physical placement of network components
 - c. Identify sensitivity to unauthorized access to components
 - d. Report observations and recommendations

Operating System Security Assessment

In a simple explanation, operating systems are the logic, rules, and code that allow the hardware to interact with an application to make it run. When purchasing a processor or PC, it must come with a brain or set of instructions — the operating system. For PCs, examples of operating systems are Mac OS, MS DOS, and Windows. In the distributed computing environment, two of the most popular and competing operating systems are Windows NT and UNIX. This section focuses on Windows NT for the sample operating system assessment. The organization, however, should perform security assessments on each of the operating systems that it uses for critical applications. Other examples of both platform and network operating systems include — but are certainly not limited to — Novell Netware, Banyan Vines, DOS/VSE, OS/2, MVS, VMS, and Solaris.

Windows NT

To understand security in the Windows NT operating system, it is necessary to understand the way NT is designed. Windows NT stands for “New Technology” and provides portability, scalability, distributed processing, and multi-user access. Windows NT runs on several architectures, including

INFORMATION SECURITY ARCHITECTURE

complex instruction set computer (CISC) and reduced instruction set computer (RISC), giving it its portability. The ability to run NT on single processor, multi-processor, and multiple processing systems provides scalability. It supports both application and network services to include databases, Web servers, and print and file services. Networking is built into the operating system itself and supports a number of transport and network layer protocols, including TCP, UDP, NetBEUI, SPX, IP, IPX, and ICMP. These protocols allow interconnectivity between Windows NT and Novell machines, SNA networks, and local Windows-based machines.

To date, Windows NT is offered in the following software versions:

- Windows NT Server 3.51
- Windows NT Server 4.0
- Windows NT Server Web Services (IIS)
- Windows NT Server Enterprise Edition
- Windows NT Terminal Server Edition
- Windows NT Workstation 3.51
- Windows NT Workstation 4.0

It is necessary to understand how the security features and configuration of Windows NT are utilized for a given installation in order to effectively review or audit NT security. Entire books have been written about Windows NT security. It would be wise to provide a copy of the latest and greatest book on NT Security to each system administrator for enterprises whose operating system of choice is Windows NT. This section provides an overview of the security architecture and considerations necessary in building a secure Windows NT operating environment.

Windows NT was designed to achieve the federal government's National Computer Security Center (NCSC) C2 rating. The NCSC rating system defines criteria to design, build, operate, evaluate, and certify trusted systems. Once a system achieves a rating according to these governmental criteria, it is listed on the Evaluated Products List (EPL) and can be purchased by government agencies requiring these levels of certification and security for operation of their systems. An EPL is available on the Internet at the following address: <http://www.radium.ncsc.mil/tpep/epl>. The Class C2 evaluation criteria is the minimum security rating required by many government agencies and offices, including branches of the military, IRS, the Federal Reserve, and certain intelligence agencies. Many nongovernmental agencies require "trusted" systems as well, and also follow the NCSC evaluation criteria. With the C2 rating, Windows NT becomes more marketable to both governmental and nongovernmental organizations requiring secure operating systems.

There are several issues that need to be understood about the security evaluations and certifications related to Windows NT. It is necessary to understand where the C2 rating comes from and what it represents. In

addition, it is necessary to understand what features and which products of Windows NT meet the C2 evaluation criteria.

The National Security Agency (NSA) has published a series of books related to evaluating and certifying trusted systems. This set of books is called the “rainbow series” because of the color of each book cover in the series. Within the series, The Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) is frequently referred to as the *Orange Book* and establishes the requirements for A-, B-, C-, and D-level secure products. The C2-level, as discussed related to Windows NT, refers to a set of security policies that define how a secure system operates.

The *Orange Book* divides security into four main classes (A through D) and several subclasses as follows:

- Class A1 (verified design)
- Class B3 (security domains)
- Class B2 (structured protection)
- Class B1 (labeled security protection)
- Class C2 (controlled access protection)
- Class C1 (discretionary security protection)
- Class D (minimal protection)

Class A is the most stringent classification and represents “verified protection.” For specific systems that have been evaluated, verified protection indicates that a specific system and its configuration has gone through stringent tests and its security has been “verified.” The distinction between level B and C relates to “access control.” In Class B, security levels or classifications need to be defined for data. An example classification may be secret or top-secret data. In Class B, this is known as a mandatory access control (MAC) system. The owner cannot use discretion about who has access to the information, but must follow mandatory rules based on the data classification. The owner cannot grant access to top-secret information to a person who does not maintain a top-secret clearance. Access is not at the owner’s discretion, but is mandated by virtue of a classification scheme. Level C2 represents controlled access protection and is defined by the owner of an object. It is called discretionary access control (DAC). Owners of objects in these type systems have discretion on who or what process accesses the owned object. The definition of a classification system for data is not specified or even necessary. Classification D, “minimal protection,” is the least secure and is typically reserved for systems that fail to meet the specifications defined in Classes or Levels A through C. Level D does not list specific evaluation criteria.

Evaluation and certification are two separate and distinct processes. Certification applies to a particular installation, including the hardware and software configuration and the operating environment of the system.

An organization or site must pursue certification on its own. As of August 1995, the NSA granted the C2 security rating for Windows NT Server and Workstation version 3.5 with Service Pack 3 (without networking installed). These products are listed on the EPL and can be accessed at <http://www.radium.ncsc.mil/tpep/epl>. It should be noted that this C2 security rating for these Windows NT products are for stand-alone systems only. Criteria from the *Orange Book* are used to evaluate commercially available, stand-alone systems. The NCSC has evaluated Windows NT as a stand-alone system, which means that as soon as Windows NT becomes part of a network, it can no longer be said to provide Class C2-level security because the evaluated configuration does not include a network environment. The *Orange Book* was written with the concept of a benign or mildly harsh environment.

The *Red Book* evaluation in the “rainbow series” extends the rating structure of the *Orange Book* to include network systems. Microsoft designed the architecture of Windows NT to be in compliance with the criteria for *Orange Book* C2 certification, including *Red* and *Blue Book* compliance. However, the C2 rating applies only with networking uninstalled. The Windows NT products have not been rated under the *Red Book* criteria. The *Red* and *Blue Books* were produced to expand upon the general requirements documented in the *Orange Book*. The *Red Book* interprets the *Orange Book* in relation to networked systems, and the *Blue Book* interprets the *Orange Book* in relation to subsystems.

The criteria listed under the NSA *Orange Book* C2 rating include:

- Discretionary access control (DAC)
- Object reuse
- Identification and authentication
- Auditing capabilities

The NT security architecture meets the C2 rating criteria by providing a trusted computing base (TCB), an object-oriented architecture, and access control lists (ACLs).

The Windows NT trusted computing base (TCB) prevents users from accessing core instructions and memory within the operating system by separating the hardware instructions into two main areas or modes: the user mode and the kernel mode. The user mode allows ordinary users to only access a separate set of processes and instructions from those of the inner operating system or kernel. This is different from MS/DOS and Windows, which allow a user to gain access to and alter the operating system with an editor or through Windows Explorer. The integrity of the operating system provided by the secure kernel provides the basis for the TCB. If an operating system can be accessed and altered, the security features are not considered effective and the requirements for C2 certification are not met.

Object-oriented (OO) architectures provide security by defining objects and the processes, methods, or software routines that are allowed to occur on those objects. Objects can include data, files, directories, disk drives, printers, resources, users, computers, and other software routines. Essentially, the object is tied to the operations or methods that can be performed on it. In user mode, access to the object can only be achieved through those processes that must be validated by the object manager before they can be applied to the object. The object manager in Windows NT is called the local security authority (LSA). Security in the OO environment is ensured because the process and methods applied to the object are pre-defined or “identified” in a database, the Security Account Manager (SAM) database, and “authenticated” before access or manipulation of the object can occur. These features of OO meet the C2 requirement for identification and authentication.

Windows NT provides security for objects through the following mechanisms:

1. *Owner*: identifies the owner of an object. The owner manages the security attributes for the object. Each owner security ID (SID) is unique and is generated for each new user that is defined.
2. *Group*: indicates the object’s group SID. This identifies which group the object belongs to and inherits security attributes from this group. The object inherits the group’s security attributes. This eliminates the need to set up specific access rights for each object or user.
3. *System access control list (SACL)*: defines the auditing feature and defines what access to the object will be recorded in the system audit log.
4. *Discretionary access control list (DACL)*: where the access rights for the object are defined. The DACL identifies what IDs can have access to an object and the type of access or security level. ACLs are made up of specified permissions or access control entries (ACEs). Access and security levels include no access, full control, take ownership, (R)ead, (W)rite, e(X)ecute, (D)elete, and (P) to permit changes to file permissions.
5. Other access controls include the ability to access a computer from the network, to log on locally, change the system time to take ownership of objects, and to shut down the system. Specific account restrictions that can be placed on a user include password restrictions, log-on times, remote access capabilities, group memberships, intruder detection/account lockout, and user-specific profiles.

The owner SID, group SID, DACL, and SACL are all contained and described in the security descriptor.

INFORMATION SECURITY ARCHITECTURE

The C2 criteria to limit object reuse means that the operating system must protect objects so that they are not randomly used by other processes, and the system must protect itself from external interference or tampering. The log-on process in Windows NT meets the C2 security requirement for object reuse, which indicates that no information should remain available in any object that has been released back to the system. To do this, memory is initialized with zeros after a process is finished and before it is allocated to a new process. The log-on process calls for a user to enter CTRL+ALT+DEL (also known as the secure attention sequence [SAS]) and protects against Trojan horses and password stealing. This set of commands terminates any processes that are running. The user is prompted to enter his user ID and password which, through the local security authority (LSA), is compared to the information contained in the SAM database. The SAM returns the SID to the LSA, which generates a security token using the SID, user name, and group access information. The NT Explorer Shell opens with the access token attached.

Discretionary access is based on the ownership model that provides an owner for each secured object. That owner specifies security attributes for the object, which include the operations and processes that may use or have access to that object, as well as who can have access and how the object is to be accessed. Discretionary control is achieved through access control lists (ACLs). ACLs are lists of users and groups that have some level of permissions to access or operate an object. These security rules in Windows NT are evaluated by the security reference monitor (SRM). The SRM is responsible for enforcing all access validation and audit policies to protect all system objects from unauthorized access and modification. The SRM compares a user's access token to an ACL for each object to determine users or groups that have privileges to that object. The SRM then generates messages according to the audit policy that gets written to an event log.

The Windows NT File System (NTFS) is the mechanism that allows the owner of an object to establish discretionary access control. NTFS also provides physical security to the NT server, secure erasure, and speedy and secure recovery from disk failures. Secure erasure ensures that users cannot read free space. The file system contains a master file table that logs information stored on the file system. Periodic updates to the log file clear it of all but incomplete transactions, committing other information on the log to disk and providing the ability to recover quickly from system crashes. NTFS is the file system recommended for effective security. Files located on file systems other than NTFS (such as file allocation table [FAT] file system in MS/DOS and Windows) and accessed on an NT system cannot be secured by the security mechanisms developed for NT and the NTFS. In NTFS, the top of the file structure is the root directory. Privileges granted at the root directory are automatically propagated to the files and subdirectories subordinate to it.

This property is called inheritance and is a feature of the object-oriented architecture of Windows NT. Unfortunately, the default ACL for the root directory of NTFS partitions is to grant full control privilege to everyone. This ACL is inherited by each file, subdirectory, and files in each subdirectory unless it is specifically changed.

Identification and authentication requires that a protected mechanism be used to verify the identity of a user requesting access. This is typically in the form of user ID and password. The log-on process with user ID and password has already been explained for local machine log-on. Network domain account log-ons use a nonce, or 16-bit, one-time randomly generated challenge packet from the primary domain controller (PDC) that is encrypted with a hashed password. In Windows NT, the operating system permits the definition of minimum password length, minimum and maximum periods of password use before forcing password changes, forced password changes for first-time log-ons, and requires a certain cycle time before passwords can be reused. Windows NT is designed to interface with PCMCIA cards, device drivers, and hardware to provide two-factor authentication with one-time password tokens and smart cards.

Audit trails must be secured and provide a record of events for all protected objects and critical events. Audit policy controls what and how much will be recorded to the audit logs. The system access control list (SACL) defines what access to the object is logged to the audit trail. Audit trails and logs are not accessible to or modifiable by users of the system, and are stored within the secure kernel, thus meeting the C2 criteria for secure auditing capabilities.

In a networked environment, Windows NT systems are organized into domains for security administration. A domain is an associated group of Windows NT platforms that share a security accounts manager (SAM) database and single security policy. The server housing the SAM and security policy is the PDC and is responsible for responding to access control issues and security questions of the platforms within the domain.

Unfortunately, Windows NT security appears to be easy to implement, but in reality presents a difficult challenge due to the complex nature of network computing and its security-related exposures. These exposures can be mitigated with the proper combination of Microsoft Service Packs, Hot Fixes, and appropriately configured firewalls and host packet-filters to block out dangerous incoming service requests. Too much emphasis should not be placed on C2 certification. This certification was designed for systems with no external disk drive and no network connectivity. In today's operating environment, this is impractical. The Windows NT Assessment Workplan can be found in Appendix B-4. A review of the Windows NT environment should include an assessment of the following:

INFORMATION SECURITY ARCHITECTURE

- Security policies
- System configuration
- System change control
- Domains and trust relationships
- Networking
- Remote access
- Physical access
- Log-on and log-off controls
- User management
- Group management
- Password management
- Directory and file system security
- System privileges and utilities
- Maintenance and operations
- Auditing, logging, and monitoring
- Backup and recovery
- Security administration

A Windows NT operating system evaluation needs to take into consideration the true operating environment, including network and Internet connectivity, organizational policies, standards and procedures, physical and monitoring controls, availability, and the realistic risk associated with the applications and information being processed by the organization. Only then will the organization be able to determine if the security related to Windows NT implementation is meeting the security needs of the organization.

Telecommunications Assessments

LANs, WANs, Internet, and microwave all are classified as telecommunications. In industry, however, these components are most frequently referred to as networks, data networks, or digital networks. The term “telecommunications” in an organization most often refers to the processes that use the analog voice networks. Those historic analog networks or plain old telephone systems (POTS) are now being migrated to digital systems. Nonetheless, the term “telecommunications,” when used, is most often referring to the voice capabilities of an organization, such as private branch exchanges (PBX), central exchanges (Centrex), key systems, mobile communications, automatic attendants, 800 numbers, calling cards, and teleconferencing and voice mail systems.

An assessment of voice systems is important and very frequently overlooked. Billions of dollars are lost each year related to exploited and unauthorized use of telephone systems.

A key control that catches such exploitations is the review and proper chargeback of telephone expense. The telecommunications department

controls the logs related to its telephone switches. These logs and reports must be broken out appropriately so that each department or business unit can review its own charges. Many organizations do not track this expense well and are unaware of their losses. If managers adequately review their monthly telephone expense figures for reasonableness, this management review provides the compensating control to identify when telecommunications fraud may be occurring. What is not reasonable? Spikes in charges and a concentration of expense consistently on specific lines raise a red flag and should be further analyzed for appropriateness.

Often in this analysis, the outcome will show a necessity for a business unit, department, or specific individual to make frequent and authorized long-distance calls. Analysis of call patterns and charges will show a consistency for the high-usage departments, extensions, and lines. It is when an inconsistency occurs that further analysis may be necessary.

Taking a baseline of call patterns is necessary to establish what is appropriate. A baseline assessment of calls consists of a more in-depth assessment of to where the calls are being made, who is making the calls, to whom the calls are made, and when the calls are made. Once this has been determined to be reasonable, deviations from this call pattern will indicate the requirement for another in-depth look at the call specifications. Tracking call patterns and charges in conjunction with management's review of charges are most often the mechanisms that catch and correlate the red flags to an actual security breach or infraction of policy.

Most common carriers now offer call detail record (CDR) exception analysis and carrier alert services to detect fraud related to phone card charges and call patterns. Telecommunications personnel should inquire about what services and analysis are available. The larger carrier services are Sprint GUARD, MCI Detect, and AT&T NetPROTECT.

When telephone charges are not tracked appropriately, employees are often aware of this and tend to pass off personal long-distance calls to the organization. If a written policy regarding personal calls does not exist and has not been explained to the employee, it will be difficult to hold the employee liable. The effect on the organization is twofold: the cost of the call and the idle time of the employee. For these reasons, it is necessary to ensure that the management and technical controls surrounding the voice system are effective. Calling privileges — or class of restriction (COR), class of service (COS), and facility restriction levels (FRLs) — can be assigned to limit calls out from the PBX. These privileges can be assigned, by extension or station number, to incoming calls and appropriate authorization.

The administrative controls related to the assessments previously described are very similar. They are designed to analyze whether enough human resources are available to cover the functions necessary for

INFORMATION SECURITY ARCHITECTURE

appropriate operation of the component. This is key from a security perspective because if there is a shortage of personnel, day-to-day operations will override the concern for security every time. The assessment workplans reviewed thus far have the following common elements:

1. The number of individuals assigned to perform the job function is adequate.
2. Responsibilities are defined and documented.
3. Policies and standards related to the functional area are defined, documented, and in compliance.
4. Documentation of component configurations exists and is accurate.
5. The use of third-party vendors to perform management and security functions of the component may introduce security concerns.

The number of individuals responsible for the telecommunications function needs to be adequate to cover all responsibilities, including security and fraud assessment. Policies and standards related to telecommunications need to include:

- A value statement regarding telecommunications assets
- A policy objective statement, which should include protecting the organization from intrusion, theft, misuse, abuse, or destruction through unauthorized access or use
- Employee access privileges are in keeping with their job assignment and responsibilities
- Employees are responsible for knowing how to operate the system properly, identifying and reporting fraud, misuse, or system abuse

System documentation related to phone lines and voice systems should include stations, or extensions, trunk groups, circuit inventories, system parameters, FRLs, COS, and COR. Documentation of current configurations provides a means of tracking and auditing when hackers have modified system configurations.

When organizations are too small to manage their own telecommunications department or equipment, third-party contracts are employed to supplement resource requirements. Security requirements need to be written into the contract to ensure that contractors follow appropriate policies and procedures related to keeping the systems environment secure. This includes policies related to passwords, access, maintenance, and change management.

The most common problem seen with third-party management is that the contractor will use the organization's name as the password to the system. This is simply for them to associate the equipment to the client, but is a significant exposure to the company. It is difficult to modify existing contracts to require third-party service providers to follow prescribed security requirements. When contracts are renewed, ensure that clauses

related to secure operations are added. One way to maintain the security of the PBX is to provide the password to the contractor when the requirement to access the system is necessary and then change the password once the work has been completed. This will require that the help desk or support personnel be available when maintenance is to be performed or as emergency restoration procedures are required.

Many third-party vendors that provide management of network and voice systems will not allow the client to access or view the configuration of that system. The reason cited is that through the contract, the service provider is responsible and liable for that connection and the configuration. Allowing individuals from the contracting organization to also have access dilutes the vendor's ability to control the environment. While this is a valid argument, it does not explain why specified individuals within the organization cannot have read-only capabilities to validate configurations and monitor changes in configurations. This requirement should also be written into the contract. Third-party service providers should follow prescribed change management procedures when making configuration modifications. This allows the organization to be able to document and monitor these changes.

Stringent physical security of phone and wiring closets is essential. In several years of performing telecommunications audits, a significant finding was that the PBX and wiring closets remained unlocked or were located in areas with uncontrolled access. Main distribution facilities (MDFs) and intermediate distribution facilities (IDFs) should remain locked at all times and be located in low-traffic areas with controlled access, which includes logging all individuals granted access, the time of access, and the reason for access. Protection against fire, flood, and temperature changes is a consideration as well.

System reports and telephone logs contain sensitive information. Proper storage, distribution, and disposal should be documented in the SS&PM. Company telephone lists are also sensitive and should require controlled distribution and be destroyed when outdated or no longer required.

Passwords for PBXs should be treated as any other computer system password. One other key finding in telecommunications reviews is that default passwords are not changed when new PBXs are installed. Password parameters and changes for PBXs need to be in line with the corporate policy for all other computer system password parameters. This includes a minimum of six characters containing both alpha and numeric characters, changes to passwords monthly, and if not feasible, quarterly at a minimum.

Remote access or Direct Inward System Access (DISA) allows a caller to dial into the PBX and access other services such as voicemail, auto-attendant systems, and outside lines to make long-distance calls. Remote access calls

INFORMATION SECURITY ARCHITECTURE

are difficult to control and associate specific cost allocations. Liability for exploitation of this service is unlimited. Replacing remote access or DISA with calling cards for specified users limits fraud liability to \$50 per card and provides an audit trail to tie cards to a specific user.

Voicemail systems need to include passwords and provide for system lockout after three unsuccessful log-in attempts. Restrictions should be placed on the ability to break out of the system to make an external phone call.

The Telecommunications Security Assessment Workplan listed in Appendix B-5 includes appropriate questions and issues related to telecommunications assessments to provide an understanding of the security posture of the telecommunications management and administrative function. Technical audits of the switch and voicemail system are best handled by trained telecommunications personnel who understand the equipment, configuration, CDRs, reporting features, and functionality of the system. Contact the telecommunications department or individuals responsible for telecommunications contract services to understand when the last detailed review of the system was performed and the objectives of that review. It is strongly recommended that if no review has taken place to date, that one be scheduled as soon as possible.

SUMMARY

Security baselines provide the mechanism for understanding the level of risk that exists within an organization. Assessments provide a snapshot of how the organization is positioned to protect itself and respond to security exposures, issues, and incidences. Security baselines should be performed on all components of the operating environment. Initially, a high-level assessment should be performed to gain an understanding of the management of the systems environment. This assessment should include a review of the operating environment, security organization, security planning, administration and management, information security policies, standards and procedures, information security risk assessments, and information classification and control. The high-level overview provides an understanding of the level of effort and priority that has been placed on security within the organization. This review should also include programs and procedures related to security monitoring, computer virus controls, microcomputer security, compliance with legal and regulatory requirements, and computer operations. Organizational controls within computer operations should be evaluated for physical and environmental security, computer systems management, access controls, backup and recovery, and problem management.

The more detailed assessments include a review of each of the components of the operating environment: applications, databases, networks, operating systems, and telecommunications. If an organization has five

critical applications, each of these applications should have its own review. Based on the level of risk and the criticality of the system, follow-up reviews should be performed to record and evaluate changes in risk, configuration, and controls. Security baselines and follow-up assessments are necessary components in understanding and protecting the organization's information processing assets.

Notes

1. Pass phrase — a phrase that combines words without spaces between the words so that the phrase cannot be easily guessable or cracked using a password cracking program. Password cracking programs attempt to crack the password by running words listed in a dictionary against the password file. Examples of pass phrases are “runhome,” “redbanana,” “sand&sun.”
2. Password cycle time reduces the ability of a user to cycle quickly through the passwords and circumvent the password history file. For example, if a password change is forced and a user wanted to keep the current password, the user could change his password ten times in one minute until he has overwritten the password history file, storing the ten latest passwords. At the eleventh password change, the password in use before the forced change is no longer maintained in the history file, so the user can change it back to what it was originally.

Chapter 5

Security Awareness and Training Program

Awareness and training are perhaps the most significant elements in an information security program. The Security Awareness and Training Program (SA&TP) is designed to help reduce the risk of losing intellectual property and processing resources. The responsibility to protect these resources is transferred to each individual in the organization through this program. To be successful, an awareness program needs to be multi-faceted and consistent with the predominant enterprise culture. It also has to be fun.

PROGRAM OBJECTIVES

The objectives of the security awareness program and the means for achieving those objectives need to be clearly understood. The objectives need to include that:

- Employees recognize their responsibility for protecting the enterprise's information assets
- Employees understand the value of information security
- Employees recognize potential violations and know who to contact
- The level of security awareness among existing employees remains high

Employees Recognize Their Responsibility for Protecting the Enterprise's Information Assets

Too often, it is assumed that employees understand the consequences of lost, stolen, or destroyed information. This is not the case. Employees tend to focus on what their particular responsibilities are within the enterprise. Most employees, if asked what are the strategic business objectives of the enterprise, would reply, "to make money." They do not realize that other objectives may include to produce quality products, to be the industry leader, to have 70 percent of market share, or to penetrate global markets. Employees contribute to those objectives by following the standards and procedures outlined for them to perform their job. Unless someone ties those standards back into an objective such as producing a quality product, employees will not be aware of that connection. The same is true for information security. It may be a corporate objective but until the

employees are told the who, what, where, when, why, and how of information security, they are only there to do their job. Information security must be presented to them as a function of their job.

One major bank clearly ties corporate objectives to information security and the employee's job responsibility in a video presented to new hires. The video introduces one of the corporate objectives as providing exceptional customer service and satisfaction. The video further explains that customers expect that their financial and personal information will be held in strictest confidence. Providing customer confidentiality and privacy is the job responsibility of the employee. Once this tie is made, the video then reiterates the main points of the information security policy. This example demonstrates the employee's first introduction to information security and his or her personal responsibility to uphold the policies and programs outlined by the organization.

Tying security responsibilities to the job description is another first step in having an employee understand the importance of information security and the concept of ownership for it. The employee's manager will review the job description with the employee when hired and again on an annual basis during evaluations. The manager is responsible for ensuring that employees within his scope of management are aware of and fully understand all information security policies, standards, and procedures.

Employees Understand the Value of Information Security

The next step is making the employee understand how information has value and that personal, legal, and financial losses as well as damage to reputation can occur if the information is not properly protected. Classification of information is one way to analyze the value of information and provides, to some degree, user awareness about its value. This awareness occurs with the information owner or business unit manager responsible for assessing and classifying the information he "owns." Labeling information as sensitive or confidential also brings about awareness of the information's value to employees authorized by job function to handle that information.

The value of information is best conveyed through real-life examples that relate to how most employees operate. A private production company put together a video for a high-visibility aerospace firm that was also a defense contractor. Admittedly, information security was a priority within this organization due to the prevalence of both corporate and international espionage. This video was developed in the Cold War era when the "Star Wars" defense plan still existed. Nonetheless, this video is extremely effective because it incorporates the everyday thoughts of the employee who begrudgingly had to perform a security function that was going to take time away from what she felt was important.

The video incorporates humor as well. The opening clip targets anti-virus scanning. It shows an employee turning on her computer in the morning and silently complaining to herself about how long the anti-virus scanning program would take to execute. This employee decides to cleverly disable the anti-virus network loadable module (NLM) and eliminate the scanning program altogether. Very proud of herself and her accomplishments, this employee hurries off to get a cup of coffee and talk with some colleagues. The video advances to later in the day when the employee starts to have trouble with one of her classified engineering spreadsheets. The video shows a big green worm chomping across the screen, eating the information, and periodically winking and laughing at the employee. To emphasize another security issue, the employee had not backed up her information, so her vital spreadsheet was gone!

Instead of complaining about necessary security functions whose ultimate purpose is to protect the employee, the employee's work, and the organization's information and processing assets, it makes sense to find more efficient processes that will allow the employee both the opportunity to perform security functions as well as the time to perform the job. The security video later shows the clever employee, coming in early to work, agreeably turning on the computer and logging in, and then going to get a cup of coffee. The video's intent at this point is to show that the employee understands the anti-virus scanning program's purpose and the risks related to not having it. The video also implies that the employee is content reordering her morning routine while the scan is being performed. There are always other things one could be doing while a virus scan is taking place. Getting a first cup of coffee is one; listening to voicemail is another.

The second part of the video deals with suspicious or unknown individuals standing around in the vicinity of the employee's workspace. The video shows the employee not turning off the computer for lunch and later forgetting to log out when leaving for the day. As the employee leaves the parking lot with his carpool, he silently contemplates if he accidentally left his computer logged in. Thinking back on his day, he remembers an unfamiliar person hanging around his workspace. He begins to imagine that the suspicious individual has returned to his desk and, because he did not log out, begins to access critical company information. In the middle of his imaginings, he spins the car around, to the shock of his carpool buddies, and returns to make sure that he has logged out of his computer. This second video theme emphasizes "doing the right thing," even when a car full of employees, anxious to get home, make that decision doubly difficult. This employee's contractual and moral obligation was to protect company assets through set standards and procedures; that is, logging out of the computer at the end of the day.

INFORMATION SECURITY ARCHITECTURE

This example video is captivating and funny and it includes realistic thoughts and feelings that the majority of employees can relate to: time-consuming virus scans and appropriate log-out procedures. It is one thing to read what one is supposed to do in a policy; it is much more fascinating to watch a video that plays out the consequences of not performing some required function.

People take so much of their lives for granted. It is rare for anyone to understand the value of information and processing resources until those resources are no longer available or a security breach actually occurs. A video allows people to live out the consequences without them actually occurring.

Employees Recognize Potential Violations and Know Who to Contact

Key to educating a user is making that user aware of the warning signs to look for that indicate a potential security breach. Human nature makes most of us trusting. When someone unfamiliar is walking alone around the office, it is not typical that anyone would walk up to him, ask him who he is and if he needs help. People are usually too busy and do not want to get involved, or just assume the individual is there for a reason and it is none of their business. This situation is very common in larger organizations where it is unrealistic to know all of the employees.

INCIDENT. Several years ago in a large international accounting firm, it was common for consultants to report to work in other cities and take over a free desk without having much contact with the employees or staff local to that office. This was acceptable and unquestioned because work was typically performed at the client and the majority of consultants were on the road and did not reside in a permanent space in the office. A nicely dressed young man began to show up for work in a professional business suit. Because out-of-towners in the office were many, no one questioned who he was or where he worked. The young man would come in, walk down the aisles and halls, and few people paid attention to him until laptop PCs started to disappear around lunchtime.

This was not an isolated incident but occurred in several different accounting firms across the country. The process for out-of-towners quickly changed and they were required to check with the reception desk and be assigned a work area. Employees were taught to question anyone unfamiliar about who they were and what assistance could be provided to them. After these informal training sessions, staff were also made financially responsible for any losses of company resources. This added incentive made the disappearance of laptop computers much less frequent.

A second incident type occasionally occurs in the healthcare industry. In the obstetrics ward of a large medical center, an individual donned a

medical scrub outfit, walked into the nursery, and walked out with a newborn infant. Because the individual appeared to know what she was doing and was dressed appropriately in hospital attire, no one questioned who she was or where she was taking the infant.

The infant was eventually found. However, procedures changed very rapidly at this hospital. A guard was posted at the entrance of the obstetrics ward and no babies came in or went out without very clear authorization. This incident cost the hospital a great deal of money, in both a lawsuit and in new procedures resulting in the necessity of a full-time guard. Hospital management could have taken preventative measures and trained its employees of risks, potential threats, and what to be on the lookout for. Management also could have implemented procedures to control access and the flow of traffic to the obstetrics ward. If training and procedures were in place, it is quite possible the incident would not have occurred and the expense of a full-time guard would not have been necessary.

Too often, people do not understand what the risks and potential costs are until they become the victim of an incident. There are four common threads to these two separate incidences that occurred in two very different industries:

1. The perpetrators were dressed appropriately for the environment.
2. Both incidences occurred during normal operating hours.
3. No formal procedures were in place to identify unfamiliar personnel operating in the area.
4. No formal training had been given to the staff in either case.

Risks are different for each industry: the loss of an infant, the loss of a PC with sensitive client information, or the loss of classified information related to a national defense program. The security program to minimize these risks, however, should have the same structure regardless of the industry or the risks: understand and appeal to human nature, identify and train on realistic risks within the industry, train individuals to know what to do to prevent those threats from occurring and to know what to do once they have occurred, and provide the necessary resources to accomplish the objectives of security awareness.

Forms of Attack. Corporate espionage can be conducted in many ways. Infiltrating the company through temp agencies and posing as a consultant is one common method. Often, espionage conducted in this way can be on the fringe of legal. Temps and consultants are often not taken through the stringent procedures of employee checklists, policy review, and acknowledgment and security awareness training simply because they are on-site for a limited time and are performing a specific function. If in fact they are not made aware of confidentiality agreements and the policies designed to educate and protect the company from exposures and are not bound by an acknowledgment

form, the perpetrator can plead ignorance. The company is held accountable for failing to take appropriate measures to protect its assets.

Technology has made it much simpler to exploit corporate secrets. The Internet was started as an experimental network by university researchers and DARPA, the Army's research agency. University researchers and educators are strong proponents of sharing information in order to accelerate discoveries. The Internet was the perfect forum for universities to achieve this objective. One company working with university researchers on code development for a software product discovered that the algorithms for the software code had been published on the Internet by the university researchers before the company could get its software product to market.

Usenet chat rooms are the perfect target for legal information-gathering and widely used for corporate espionage. Usenet chat rooms are a forum for electronically talking with others that have a similar interest. Unwittingly, corporate and academic researchers as well as individuals with detailed knowledge about a particular subject matter will inadvertently answer questions in chat room sessions. What was once used primarily to accelerate research in a positive way is now being used to exploit that honorable objective for personal gain.

There are many security consultants that provide searches of the more infamous hacker Web sites to determine if the company is a specific target. It is commonly known that Microsoft is a particularly visible target for both corporate espionage, as well as disgruntled users of other operating systems and software products who are not particularly pleased with Microsoft's overbearing market presence.

Another technique is called "dumpster diving." Individuals are paid to collect the trash from technology firms and corporations that have trade secrets to protect. Temps, disguised consultants, cleaning crews, and disgruntled employees have easy access to the wastepaper baskets of important and knowledgeable corporate personnel. This has been one of the most common methods of espionage prior to the advent of distributed computing and still exists because it is easy.

Corporate espionage has increased to the extent that a professional society now exists for those specializing in intelligence-gathering against their competitors. William Holstein's article, *Corporate Spy Wars*, in the February 23, 1998, issue of *U.S. News & World Report*, describes The Society of Competitive Intelligence Professionals as an organization with over 6400 members. Society membership includes representatives from some of the largest U.S. companies that compile psychological profiles of senior executives, track financial filings with the Securities and Exchange Commission, order satellite photos to spot factory expansions, and monitor patents and research papers as they become available. They also review blueprints

that must be filed locally for building permits, taxes, and infrastructure support through the local fire department. Holstein's article lists some of the more common intelligence-gathering sites as:

- Corporate information — <http://www.corporateinformation.com>
- Securities and Exchange Commission — <http://www.sec.gov/cgi-bin/srch-edgar>
- Newsworks — <http://www.newsworks.com>
- Inquisit — <http://www.inquisit.com>
- The Monster Board — <http://www.monster.com>
- Tierra Highlights2 — <http://www.tierra.com>
- Dejanews — <http://www.dejanews.com>
- IBM Patent Server — <http://www.patents.ibm.com>
- Virtual Library — <http://www.dut.com.tr/lists/W3VirtualLibrary/Overview.html>
- Northern Light — <http://www.nlsearch.com>

If corporate espionage is highly probable in an organization, it would be an effective security countermeasure to scan these sites to understand what may be out there that can be used for intelligence-gathering against that organization.

In developing an effective security awareness program, it is necessary for employees and users to be aware of pertinent laws and regulations regarding their conduct at work. Legal counsel within the organization should assist with the development of a security awareness session targeted at employee conduct and the pertinent laws and regulations supporting that conduct.

Below are listed some common topics that should be included in user awareness and training sessions:

- Security policy (e-mail, Internet)
- Confidentiality, integrity, and availability
- User ID and password requirements
- Appropriate use of resources
- Virus scanning and reporting
- Shoulder surfing
- Social engineering
- Use of encryption
- Individual responsibility
- Information classification and handling
- Threat by industry
- Incident reporting
- The information security organization
- Internet access guidelines
- Physical security

INFORMATION SECURITY ARCHITECTURE

- Chain mail
- Information transmission, storage, and processing
- Information security programs
- Security monitoring programs
- Verbal communication in public
- Use of cellular phones

Passwords are perhaps the most important topic of the security program. They are the keys to gaining system access. Employees should be instructed on:

- How to establish good passwords
- How passwords can be guessed or exploited
- The importance of not sharing passwords
- The importance of changing passwords frequently
- The damage that can be done from unauthorized access

Employees need to know that they play an essential part in securing systems by complying with strong password policies.

Employees also need to be made aware that it not an option to report suspected incidences. Organizations should have a Code of Conduct or Code of Ethics from which to operate. This code spells out acceptable and nonacceptable behavior within the organization. The Code of Ethics outlines the employee's moral obligation to the enterprise. One of these obligations is the responsibility to correct or report wrongdoing that could have a negative impact on the enterprise. To follow through with this obligation, it is necessary that a framework exists so that individuals can report suspected security violations and other incidents involving the security or integrity of information or information technology systems.

The Level of Security Awareness among Existing Employees Remains High

This objective is the crux of program. The SA&TP needs to target five different groups within an organization: employees, system administrators and security liaisons, security officers, department management, and executive management. The content of each training or awareness initiative will be different for each group. The security topics above are a good basis for the training of all groups. Additionally, system administrators will be required to participate in security technical training for the operating system, network, database, or application that he or she manages. Security officers will need to focus on the Information Security Architecture and its components and how those components are integrated into the SA&TP. Department management has the additional responsibility of ensuring that all employees within its span of control understand and adhere to security policies and receive security awareness training. Training for department managers should

emphasize realistic risks and consequences to the operation of the business so that managers take information security policies and training seriously. They will also be responsible for defining classification of resources within their business unit. Classification provides additional opportunities to target department managers on awareness topics such as establishing compensating controls and enforcement of policy to reduce risk. Executive management is responsible for making decisions related to security awareness and training, and will be responsible for the long-term financial commitment to the program. Training to gain buy-in should begin at this level.

It should be noted that awareness and training are two distinct methods of transferring knowledge about information security. Training is more formalized, typically in a classroom or conference setting where the objective is to gain knowledge about a particular subject. Awareness is a passive mechanism that occurs through less formal methods such as posters, themes, and objects such as key rings and cups. Both are important and, if executed properly, both can be very effective.

PROGRAM CONSIDERATIONS

To meet the objectives of the Security Awareness and Training Program, there are four things to consider:

1. Effectiveness is based on long-term commitment of resources and funding
2. Benefits are difficult to measure in the short term
3. Scoping the target audience, both new and existing employees
4. How to effectively reach them

Effectiveness Is Based on Long-Term Commitment of Resources and Funding

There must be a long-term commitment of resources and funding. Security awareness and training is not a one-time effort. All existing employees should receive training throughout the year and new employees must be trained upon beginning their employment. Some companies have made it a policy to have departing employees revalidate their confidentiality obligations to the company. Many organizations are establishing full-time positions for SA&TPs.

To establish a budget and long-term training plan, several considerations should be made, including:

- The number of locations and users in the organization
- Inclusion of third-party service providers, consultants, temps, and contractors
- Classifying attendance as mandatory

INFORMATION SECURITY ARCHITECTURE

- Integrating the SA&TP with other programs such as new-hire orientation
- Tying the SA&TP to relevant policies, documents, and standards such as the information security policy, SS&PM, Internet policy, e-mail policy, code of conduct (or ethics), and laws and regulations related to the business and industry
- Targeting both existing and new employees and the different levels of the organization: users, administrators, security officers, business unit management, and executive-level management
- The number of formal internal training events that will be conducted throughout the year
- The cost of conferences, seminars, lectures, magazine subscriptions, and professional group memberships
- The communications channels available within the organization to leverage awareness campaigns
- Security campaign items for purchase such as cups, id card holders, magnets, hats and clothing, professionally developed posters and banners, videotapes, software, and incentive awards (vacations, dinners, airline tickets, cars, show tickets, paid vacation days)

Benefits Are Difficult to Measure in the Short Term

The benefits of a training program are not tangible in the short term and can be difficult to measure in the long term. One can attempt to quantify potential benefits by revisiting both of the very real incidences described earlier in this chapter. In the first scenario in which the laptop computers were stolen, the losses are calculated as follows:

5 laptops @ \$3500	=	\$17,500 (tangible loss)
Consulting rework (200 hours @ avg. \$100/hr)	=	\$20,000 (tangible loss)
Administrative staff — to order, configure, and distribute new PCs (30 hours @ avg. \$50/hr)	=	\$1,500 (tangible loss)
TOTAL TANGIBLE LOSS		<hr/> \$39,000
Client information	=	Unknown (intangible loss)
Potential lawsuit from mishandling sensitive and confidential client information	=	Unknown (intangible loss)

From this example, part of the loss is quantifiable. If \$20,000 had been spent on a SA&TP or procedures development, the thefts may not have occurred. Tangible savings to the organization are estimated to be \$19,000.

Security Awareness and Training Program

Tangible loss	\$39,000
SA&TP investment	<u>\$20,000</u>
Tangible savings	\$19,000

Continue with the second incident related to the kidnapped infant:

Lawsuit from parents	\$500,000
Legal fees	\$100,000
24/7 protection (2 guards @ \$28,000/annual)	<u>\$ 56,000</u>
Tangible loss	\$656,000
Reputation damage	Unknown (intangible loss)
Lost clients	Unknown (intangible loss)

In this example, imagine if a \$50,000 investment in an SA&TP and some precautionary procedures had been made.

Tangible loss	\$656,000
SA&TP/procedures	<u>\$ 50,000</u>
Tangible savings	\$606,000

When an SA&TP is in place, it is difficult to know what would have happened if the SA&TP had not been in place. It is difficult to measure what has not yet occurred. Loss estimates can be formulated on previous incidences or potential incidences that are caught quickly and rectified due to proactive procedures. Comparisons can be made to incidences involving the competition within the same enterprise. If the incidence has occurred at a competitor, then more likely than not, it is a realistic threat and proactive measures should be taken to keep it from happening within one's own organization.

Scoping the Target Audience

New employees should receive preliminary training during new-hire orientation. If new-hire orientation is not a formal class, it is typically performed one-on-one by human resources or department management. In each case, the individual providing the training must:

INFORMATION SECURITY ARCHITECTURE

- Understand the security policies themselves
- Emphasize the importance of the SA&TP to the new hire
- Give the new hire appropriate time to thoroughly read and understand all policy documents
- Ensure that signatures are received on all appropriate policy acknowledgment forms

There are also two types of existing employees: those who were employees prior to SA&TP development and those who have read the policies in new-hire orientation and have forgotten what they are. Refresher training on policies needs to be performed and acknowledgment forms revalidated annually unless the following situations require more frequent training:

- All new employees who will be using the computer within 30 days of employment
- Whenever there is a significant change to the organization's information security environment or procedures
- When an employee transfers to a new position that deals with sensitive information
- As a policy refresher based on the sensitivity of information an employee handles in their job function

The training for new hires and refresher training for current employees is most efficiently offered to a group in a classroom setting. Some tips include:

- Present the security policy in a 15- to 30-minute session.
- Do not have the employees only read the policy. Provide a video and revisit the main policy points once the video has been shown.
- Use graphics that are catchy.
- Define terms like confidentiality, integrity, and availability in ways that relate to the employee's job function and must cause the employee to think about the definition. For example,
 - *Confidentiality*: Does the secretary you have lunch with every Wednesday need to know how much more money she would make if she was the executive director's secretary?
 - *Integrity*: Is the Excel spreadsheet that you have programmed to summarize the department's budget generating the correct numbers? Have you formally tested and validated them?
 - *Availability*: What would you do to perform your job if the network connection to your computer goes down for six hours?
- Remove the participants from their normal duties and conduct the training at a different location.
- Prepare an agenda in advance.
- Class preparation and planning should include the who, what, where, when, why, and how of Information Security and the audience.

One argument of security professionals has been, how much should one tell users about security. While educating them to protect the company's resources, one is also educating them on vulnerabilities and easy exploitation techniques. It is important to understand this when developing and conducting user awareness and training sessions, and it is important to provide the incentive to users not to choose the road of impropriety. By demonstrating what the company is prepared to do and does do to thwart attacks and respond to incidences, employees will begin to understand that the company is serious. One thing that one never wants to do is introduce the employees to a list of questionable Web sites dealing with corporate espionage or cyber hacking information.

Explaining to employees that the company has software that records and reviews all Internet sites accessed by an employee is a deterrent for using the Internet for personal use during business hours and for accessing disreputable sites that can cast a negative shadow on the employee and the company. Many employees have been caught downloading pornographic materials to corporate-owned computers for both personal use and to embarrass co-workers. Some Internet sites record the TCP/IP addresses of those accessing their Web site and can trace the originator back to the company. Many companies have suffered from negative publicity due to an employee accessing risqué Web sites.

Software also exists to record keystrokes. This software was developed to monitor productivity, but is now being used to target potential sources of security breaches. Use of these tools can create a "big brother is watching" mentality and is often not embraced by management because it instills a sense of distrust that can work against the corporate culture an enterprise is attempting to instill. Other deterrents are examples of management following through on disregard for policy by suspending, transferring, reprimanding, or terminating employees. A demonstration by management that it is willing to stand behind its policies provides an incentive for wayward employees to steer clear of impropriety. It is when employees do not believe that management is serious, or that there is a double standard, that they will test how far they can go or will completely disregard policies. Double standards exist when executive management asserts policies for employees yet fails to follow policy themselves. Password sharing is a common example of this. Guidelines may be established that forbid the use of password sharing and establish procedures for changing passwords every three months. This author has often run into department heads and executives who have shared their password with their secretary and they fail to change their password according to standard.

INCIDENT. A very large organization with over 30,000 employees implemented a security waiver process whereby any department not capable of meeting a corporate security policy or standard could request a waiver to

policy by presenting a solid business case. The Security Waiver Committee received a waiver from an administrator of one of the independent business units with the following business justification: “CEO and President of the Bank request that password timeouts be turned off for all systems.” The waiver was denied and returned.

Training of executive management is quite different. Executive management is responsible for approving and supporting the SA&TP. They must understand all possible and probable events that could occur if a formal training program is not implemented. If an SA&TP is not already in place, a meeting should be scheduled with the objective of explaining to executive management its scope, cost, risks, benefits, and potential cost savings. Examples and comparisons should be made to actual incidences within the same industry, either internal to the organization, from competitors, or within similar industries. It will be necessary to attempt to quantify the benefits of the program on an annual basis to ensure that program funds continue to be allocated. Just as users must have refresher training, executive management needs to be reminded of the risks, benefits, and potential cost savings of not having damaging incidences occur. These meetings are essentially the awareness and training program for executive management.

Whenever there is a significant change in the information security environment, another meeting should be scheduled with executive management to discuss the impact of that change as well as to educate executive management regarding the technology related to the change. An example of this is the requirement for encryption. Many executives do not understand what it is or why it is necessary. A meeting to discuss these issues is a part of educating executive management. Executives cannot and will not support anything that they do not understand.

Business unit management will also not support what it does not understand. One-on-one meetings with business unit management are similar to those held with executive-level management, except that business unit managers are not the approvers of the program. Emphasis should be placed on business unit risk, potential incidences and costs of incidences, and the potential savings of implementing an effective program. Business unit managers do, however, need to understand and buy into the SA&TP in order to support it and encourage department managers to support it.

Security officers are often the project managers for the SA&TP. They are responsible for developing the SA&TP Project Plan and presenting it to executive management for approval. They are usually the ones who present risk and training requirements to business unit management. Training and awareness for security officers and security administrators come from seminars, conferences, security magazines, professional group lectures, on-the-job training, and individual research. Topics for educating the security officer may include instruction on:

- Information Security Architectures
- Access control
- Single sign-on
- Security assessments
- Certification of Web sites
- E-mail security
- Internet security
- Routers and firewalls
- Network operating system security
- Threats and vulnerabilities
- Penetration testing
- EDI/EFT
- LANs, WANs, MANs, VANs
- Public switched networks
- Microwave technology
- Wireless LAN technology
- Physical security
- Social engineering
- Classification methodologies
- Encryption
- Public key infrastructures
- TCP/IP security
- Mainframe
- Distributed architecture security
- Remote access authentication
- Anti-virus
- Neural networks
- Backup and recovery procedures
- Disaster recovery planning
- Business continuity planning
- Ethics
- Law and regulation
- Industrial espionage
- Software piracy
- Software copyright compliance

There is a lot to understand in order to be an effective security officer. Most of the security officer's training will come from external sources. This needs to be made a priority in the SA&TP budget. This author frequently runs into organizations that provide their security officer with one seminar to attend a year. With the myriad of topics listed above, it would be a tough choice in narrowing it down to one. Security magazines are a key source of information and education. Some of the better known magazines are *IS Audit & Control Journal*, *The Information Systems Security Association Journal*, *Computer Security Alert*, *Info Security News*, and *Information Systems*

INFORMATION SECURITY ARCHITECTURE

Security. These journals are included in the cost of membership to organizations such as Information Systems Audit and Control Association (ISACA) and the Information Systems Security Association.

System administrators and security liaisons require specific training. System administrators are responsible for the security configuration of a particular system. These systems can include:

- Novell Netware
- UNIX
- Windows NT
- Banyan Vines
- VMS
- MVS
- Data switch networks
- Web servers
- Mainframe operating systems
- CICS
- ACF2
- RACF
- Lotus Notes
- Application systems
- Firewalls
- Voice switch networks

There are seminars for each of these systems that focus primarily on security. For larger organizations, it may make sense to bring a seminar on site so that all administrators of the same system can receive the training locally.

Effectively Reaching the Target Audience

In the previous section, the focus was predominately on the content of formal training. This section emphasizes ways to make security awareness more effective. Mandatory training that is conducted on a scheduled basis covers only a portion of the SA&TP. Awareness consists of delivering messages to employees consistently and often to get the information security ideas to stick.

Methods for delivering information security messages are:

- Executive and management presentations
- Outside speakers
- Videos and multimedia presentations
- Security slogans and messages
- Distribution of security alerts
- Computer Security Day activities
- Newsletters

- Contests and drawings
- Posters, cups, calendars, key chains, etc.

Executive and business unit management presentations were discussed in the previous section. These presentations must emphasize effects on business operations. Just as a data entry clerk's main objective is to enter as many correct transactions to achieve bonus status, a business unit manager's main concern may be excellent customer service resulting in increased sales. A presentation outside the scope of what concerns him on a daily basis will fall on partially deaf ears. The information security presentation must be clearly tied to his business goals and objectives to gain his full attention.

Outside speakers can consist of technical experts for a given system and can include more flamboyant speakers with a tale to tell. Clifford Stoll, a Berkeley astronomer, was the guest speaker at an Ernst & Young, LLP, internal training program. Clifford is a zany astrophysicist, lecturer, and author with Birkenstocks and a ponytail. Clifford traced an international hacker attempting to access highly classified government information related to a national defense initiative. He wrote *The Cuckoo's Egg*, which documents the trace and is a very popular must-read among security professionals. Clifford's stories were captivating and real. He injected a touch of insanity into his fascinating tale of the hunt.

Famous and popular speakers can be costly. Other speakers can include not-so-well-known individuals but still have a fascinating story related to the industry. Stories are effective because the listener does not perceive them as something they are required to learn but rather, something that they are enjoying and are a part of as the story is told.

Videos and multimedia presentations are also popular. A very effective method for security awareness videos is having the chief executive officer or president of the company introduce the program and talk about its importance in the video. This establishes full support for the program. Employees tend to listen more closely to the "top dog" of the organization.

If a customized video is out of the budget, Commonwealth Films, Inc., produces videos on computer security, information security, records management, disaster recovery, software piracy, and viruses. *Disaster Recovery Journal* and the *Rothstein Catalog on Disaster Recovery* produce videos on disaster recovery. Power Point presentations with colorful graphics, swooping screens, disappearing and reappearing pictures, and interesting sounds keep the audience stimulated and awake.

Security slogans and messages are a constant reminder that an active program is in place. One large bank hands out to each new employee its access card key with a bolero imprinted with the security department's slogan. The bank also uses professionally made signs that top each intersection of the office with such phrases as Encryption Alley, Password

INFORMATION SECURITY ARCHITECTURE

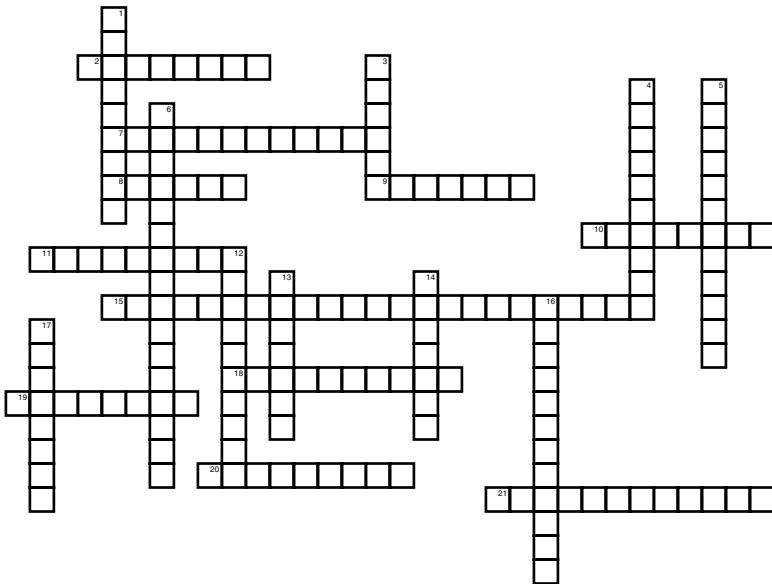
Place, Compliance Court, etc. A bit corny, but every time a visitor comes to the department, there is a visual reminder of the security program. Interactive e-mails can also be sent out as catchy reminders.

Distribution of security alerts is another very crucial piece of SA&TP. Corporate Security is the owner of alerts and should be on newsgroups and distribution lists from software vendors and organizations that offer advisory services. The Security Group should also maintain internal distribution lists to redistribute alerts related to particular topics. When a CERT, virus, or other security alert is published, it is Corporate Security's responsibility to disseminate that alert as quickly as possible to all relevant administrators. IBM has a service called IBM ERS (Emergency Response Service) that provides assessments, incident assistance, and security alert distribution. A company owned by IBM in Reston, Virginia, called ICSA, provides a Web site certification program and also includes alert notification in this service as well. The National Infrastructure Protection Center (NIPC) provides the *Awareness of National Security Issues and Response* (ANSIR) communication to corporate security professionals and others who have requested to receive unclassified national security advisories called ANSIR e-mails. Virus vendor Web sites provide alerts on the most recent viruses. Some of those vendors include TruSecure, Trend, Symantec, and Norton. Their Web sites are listed below:

- ntbugtraq@listserv.ntbugtraq.com
- <http://www.microsoft.com/security/bulletins/ms99-019.asp>
- <http://www.cert.org>.
- <http://www.cert.org/nav/alerts.html>
- <http://www.symantec.com/avcenter/index.html>
- <http://www.symantec.com/avcenter/vinfo/db.html>
- <http://www.antivirus.com/vinfo/alerts.htm#top>
- <http://www.antivirus.com/vinfo/virusencyclo/default.asp>

Computer Security Days can be fun to plan as well as effective for advancing awareness throughout the organization. If the company has a cafeteria, the entrees and items can be cleverly named and labeled. Ideas include password pasta, encryption egg salad, single sign-on spaghetti, PKI pizza, backup brownies, security stew, jailbreak jello, compliance cookies, certification salad, etc. The Security Day could include several training classes and seminars. Attendees could receive a shirt, cup, or other memento for attending. Contests for best security slogans should be offered with enticing prizes such as weekend getaways, rounds of golf, visits to the day spa, tickets to professional sports events, theater, opera, or symphony, and dinner for two. When giving away nice gifts, one will be surprised how many individuals suddenly become interested in the cause.

A semi-annual contest or raffle with larger prizes (such as a \$1000 vacation, two airline tickets to anywhere in the world, or a pair of ski-doo's)



ACROSS

- 2. Management's rule set
- 7. Phone number discovery methods (2 wds.)
- 8. Path designator
- 9. Passive information-gathering device
- 10. Accepted way of doing something
- 11. A "touchy" information classification
- 15. Foundation for asymmetric key management (3 wds.)
- 18. Personal key (2 wds.)
- 19. Blocking mechanism
- 20. Truthfulness
- 21. Validate the identity

DOWN

- 1. Method
- 3. Heads up
- 4. Within the law
- 5. Connecting from afar (2 wds.)
- 6. Start point for understanding controls (2 wds.)
- 12. Message scramble
- 13. Validate
- 14. Computer wrongdoers
- 16. It means "private"
- 17. Checking for compliance

Exhibit 5-1. Security crossword puzzle.

would entice most people to take a stab at just about anything being suggested. The contest might include completing a series of tasks related to security. For each task, an employee would receive one entry in the contest. Tasks might include reading the security newsletter, completing a computer-based training class on security, attending a training session or seminar, completing a security crossword puzzle, or taking a series of tests on security. Offering such prizes costs nothing compared to the price of an incident or recovery from an incident.

Exhibit 5-1 displays a sample of a security-related crossword puzzle that offers definitions of the more common security terms (answers provided in Exhibit 5-3). The crossword puzzle is a training aid that provides exposure and awareness to security in a light and fun manner. This sample puzzle is a mix of security terms. Crossword puzzles can be incorporated into the

INFORMATION SECURITY ARCHITECTURE

monthly or quarterly newsletter and relate to a specific article on technology. This may encourage the reader to reference the technology story when attempting to complete the crossword puzzle. An example technology article might be on public key infrastructure; related words for the crossword puzzle for this article would include:

- Certificate authority
- Vetting process
- Directory services
- Digital signatures
- Web-enablement
- Trusted root
- Key ring
- Private key
- License
- Key recovery
- Entitlement
- Nonrepudiation
- Confidentiality
- Seed

Developing newsletter articles and crossword puzzles enhances the knowledge of the individual who is responsible for researching the topic and writing about it, as well as developing a related crossword puzzle. Exhibit 5-2 is a sample newsletter that exposes employees to security programs, security personnel, policy issues, as well as more popular security-related topics or technologies.

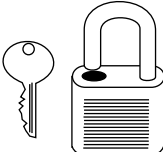
Most word processing software packages now come with templates to develop newsletters. Broderbund's Print Shop can be purchased for under \$40 and comes with thousands of pictures and templates to make several different layouts of newsletters as well as brochures. Microsoft Word also comes with a newsletter template that is simple to use. Lotus Notes is a common corporate software and can also be used to send newsletter summaries that can be linked to several documents. Lotus Notes allows one to add view-like summary information about the documents and to designate how many documents should be included in one newsletter.

Pictures and color draw attention and cause personnel to become interested in the content. This author began to produce his children's school PTO newsletter in color, and had over a dozen parents introduce themselves and say how interesting the newsletter was and how they could not wait to read it every month. Many of the parents were men who admitted that they had never read the newsletter before. The funny pictures and color piqued their curiosity. The content had not changed; it was the presentation of the information that became a draw. The PTO newsletter had a sizable impact by increasing the level of PTO participation and volunteerism. A security

A Monthly Publication of SECure TECHNOlogy Services

Security Monitor

Introducing Security Monitor
A Monthly Publication of SECure TECHNOlogy Services



What's Inside

This publication has been established to introduce you to SECure TECHNOlogy Services at Starcross, Inc. This update will provide you with security related information, issues, programs and people within the SECure TECHNOlogy Services Group.

This communication will include topics on:

- System & Network Security Information & Corporate Security
- Introductions to Technology Product Reviews
- Management Viewpoints
- Puzzles, Quizzes & Contests

We encourage you to email us at the LotusNotes address: SECure TECHNOlogy Services with your ideas of what you would like to see in future issues of **Security Monitor** and recommendations for improving the effectiveness of this newsletter.

CONTENTS

- Technology Review. . . 1
- Virus Alert. 2
- CIO Communication. 3
- Product Review. . . . 4
- Fun & Games. 5

Next Month's Issue will contain articles on:

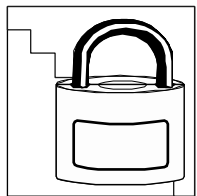
- Emergency Response: Are You Ready?
- Social Engineering: What You Should know
- Viruses: Impacts of Chernobyl and Melissa
- A Message from the Executive Committee for Security

What is the Role of SECure TECHNOlogy Services?

SECure TECHNOlogy Services is tasked with initiating programs within Starcross, Inc. to minimize the security risks and exposures to systems, personnel, information and corporate assets from theft, fraud and accidents. Security events within Starcross can result in losses of revenue, reputation, physical resources and even human life.

Find out more about who the SECTECH team is and how they can help you protect your department's assets.

This section of the newspaper will be dedicated to introducing the SECTECH staff and important security related issues.



The official logo of SECure TECHNOlogy Services

Volume 1, Issue 1 June 2000

Exhibit 5-2. Sample newsletter.

newsletter can provide necessary and useful information through an interesting and casual presentation format. It is not what one says that gets heard, it is how one says it.

Security Organizations

There are many organizations that an Information Security Officer (ISO) should join in order to receive the most recent security issues and alerts.

INFORMATION SECURITY ARCHITECTURE

The following list is recommended to ensure that the ISO is receiving the most recent information on security:

1. **Computer Security Institute (CSI)** — CSI membership costs \$197 and includes subscriptions to the *Computer Security Alert* monthly newsletter; *The Computer Security Journal*, which is published semi-annually; *The Annual Computer Security Products and Services Buyers Guide*, *Fax Alerts*, and *The Manager's Guide Series*; as well as discounts on conferences and seminars.
2. **Information Systems Security Association** — An international organization providing an educational forum, a publication, and peer interaction. The group promotes management practices that ensure availability, integrity, and confidentiality of resources.
3. **International Computer Security Association (ICSA)** — NCSA provides training, testing, research, product certification, underground reconnaissance, and consulting services for information security.
4. **Communications Fraud Control Association (CFCA)** — The CFCA promotes ways to reduce fraud through increased cooperation among the telecommunications industry, end users, and law enforcement. It provides conferences and seminars and a forum to address issues facing the telecommunications industry. A news-weekly is delivered by fax, a telecommunications journal is available bimonthly, and helpful hint brochures are sent automatically to its members.
5. **The Institute of Internal Auditors** — An international organization that promotes management practices to ensure the availability, integrity, and confidentiality of resources. Membership provides an educational forum, a publication, and peer interaction.

SUMMARY

The SA&TP helps reduce the risk of loss of corporate information assets by training employees to understand the value of information security, to recognize their responsibilities to protect it, and to recognize potential violations and report them. The level of security awareness among existing employees must remain high through a series of training classes that are supplemented with frequent reminders of the program's objectives.

The SA&TP consists of both training classes and frequent reminders of the importance of security. It is necessary to think outside the box when developing an SA&TP. Creativity plays a crucial role in drawing employees into the concepts of security. It is necessary to create a connection between the security program and how employees think and feel about performing their jobs.

The SA&TP requires planning, budget, creativity, and support from executive management. It needs to target all levels of the organization to continue

to be effective. The benefits of an SA&TP are difficult to see and quantify in the short term, but the end results can have a significant financial impact on the organization by preventing unnecessary incidences through negligence, ignorance, or willful negative behavior.

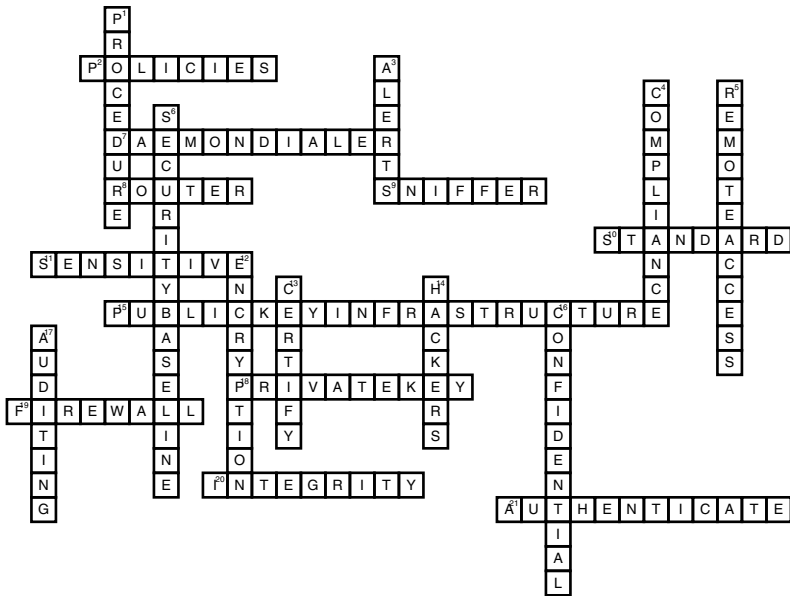
GETTING STARTED — PROGRAM DEVELOPMENT

This section is designed to provide a preliminary workplan for initiation and development of the SA&TP.

1. *Develop and schedule training targeted at executive-level management.* This training should include awareness on realistic threats to the business and examples of published or known losses internally and of competitors. This training should also include an introduction of the SA&TP plan.
2. *Assess security policies, procedures, and guidelines.* A thorough understanding of these documents is necessary for presentation at training sessions.
3. *Identify strategic information sources and mission-critical systems.* Again, sources provide the content for inclusion in training program development. Mission-critical systems and related risks to those systems should be emphasized in the SA&TP.
4. *Establish an SA&TP Committee.* This Committee should meet once or twice a month at program initiation and consist of representatives from business units as well as system administrators and members of the Security Team. The objective of the SA&TP Committee is to evaluate and recommend training efforts, identify problem areas, and review incidences.
5. *Review and recommend security tools.* The security policies and standards should outline what security tools and mechanisms will be used throughout the organization. These tools need to be reviewed by the SA&TP Committee and be included as a part of the training program so that individuals know how to appropriately use these mechanisms. Mechanisms include screen savers, encryption technologies, laptop security, remote access cards, physical security access cards, and keypads.
6. *Establish emergency and incident response and reporting procedures.* Identify contacts and phone numbers for escalation of incident reporting. Establish escalation procedures and provide training to all individuals on those procedures. Viruses are rated as the most common security incident. Training on the response and reporting of viruses requires the widest and most thorough dissemination of training throughout the corporation. Preliminary training should define what viruses are, how to recognize them, provide an explanation of the anti-virus program that has been implemented, and describe how to report a virus. Emergency and incident response of any security breach should follow this same reporting procedure.

INFORMATION SECURITY ARCHITECTURE

7. *Schedule training.* Establish a training mission by scheduling all individuals for training throughout the year. Individuals should be scheduled for training within function groups as follows:
 - a. Executive management training
 - b. Network administrator training
 - c. Middle management training
 - d. Systems administrator training
 - e. Programmer/DBA training
 - f. Mobile user training
 - g. Help desk training
 - h. General user training
8. *Identify communications methods.* Determine which communications mechanisms will work within the organization's environment. These mechanisms can include posters, newsletters, e-mail, Lotus Notes, desktop signs, brochures, flyers, and banners.
9. *Determine security awareness promotional activities.* Include in the SA&TP the necessary support for Awareness Days promotional handouts (such as coffee mugs, polo shirts, lanyards, key chains, and pens). Include large ticket item promotions such as contests for vacations, bicycles, theater, or sporting event or airline tickets.
10. *Integrate security into organizational processes.* Add SA&TP as a budget line item. Include security awareness as a topic for other organizational meetings such as status review sessions, business unit meetings, and IT planning sessions. Ensure that procedures for processing visitors such as sign-in rosters, ID badges, and escort policies are addressed by the SA&TP. This should also include processes for vendors, contractors, and temporary staff.



ACROSS

2. Management's rule set
7. Phone number discovery methods (2 wds.)
8. Path designator
9. Passive information-gathering device
10. Accepted way of doing something
11. A "touchy" information classification
15. Foundation for asymmetric key management (3 wds.)
18. Personal key (2 wds.)
19. Blocking mechanism
20. Truthfulness
21. Validate the identity

DOWN

1. Method
3. Heads up
4. Within the law
5. Connecting from afar (2 wds.)
6. Start point for understanding controls (2 wds.)
12. Message scramble
13. Validate
14. Computer wrongdoers
16. It means "private"
17. Checking for compliance

Exhibit 5-3. Security crossword puzzle answers.

Chapter 6

Compliance

Compliance measures the extent to which defined policies, standards, and procedures are being followed. Compliance includes auditing, monitoring, and investigating at several different levels of the organization. This chapter discusses the components of compliance within these levels of the organization.

At the first level, the information owner or individual assigned responsibility for the component must ensure that appropriate preventative and detective controls are in place and are being utilized effectively. Individuals at this level include information owners, component administrators, and security liaisons for the business unit or department. These individuals are responsible for the actual implementation of the controls. Controls at this level include establishing and maintaining access, implementing monitoring and alert tools, administration of audit trail reports, management review of log-in attempts, implementing security parameters, and investigation of lockouts. At this level, detection of security violations minimizes the damage done to the organization.

The second level of compliance is the audit function. The audit function can be performed by the internal audit department, external auditors, or a combination of both according to industry standards. Audit objectives include ensuring compliance with corporate policies, standards, and procedures as well as developing programs to understand the control environment, perform risk assessment, and establish control procedures. The audit function must evolve along with the organization's changing information technology infrastructure. As the organization moves to a client/server environment, controls and procedures that have historically been managed by one department can now be implemented by different individuals from different departments. For several years, auditors continued to audit application and mainframe controls, ignoring the networks and client/server systems because of the lack of knowledge and toolsets available to audit these environments. Now, key parts of audits are those targeted at the networks and distributed computing environments.

The third level of compliance is at the Security Team or Committee level. This is investigative in nature and, instead of focusing on a particular application or component, the Security Team is responsible for ensuring that security is implemented organizationwide. The Security Team or Committee

INFORMATION SECURITY ARCHITECTURE

is concerned with systemic security issues that will require management approval to implement. Examples of this include one-time password systems that will be implemented organizationwide and require budget approval. Another example is a change to the security policy in response to a significant security breach resulting in a lawsuit. The Chairman of the Security Team is responsible for ensuring that the incident is properly investigated and a resolution is discussed to minimize the risk of the event recurring.

LEVEL ONE COMPLIANCE: THE COMPONENT OWNER

Chapter 2 discussed the roles of the security owners and liaisons as well as network and application administrators. These individuals are the component owners responsible for compliance at the lowest level of the organization. The security coordinators are assigned within each location, department, and business unit to establish the security policies, standards, and procedures within the subunit and to coordinate with the department business managers on security-related issues. The coordinator's primary responsibility is to ensure that appropriate user access within the scope of their business function is maintained.

To ensure appropriate access, a procedure should be established to have component owners, network and application administrators run a listing of specified access by user on a quarterly basis, at a minimum. These reports are then submitted to the security liaison of each business function to review for appropriateness.

As stated in Chapter 2, additional responsibilities of the security coordinators/liaisons are to:

- Ensure that application access forms are initiated for existing and new users within the respective departmental area
- Ensure that access is modified or deleted when employees and non-employees (consultants, contractors, business partners) operating within their business function or site are transferred or terminated
- Conduct user security awareness within their departmental function
- Ensure that the enterprise Confidentiality Agreement and exit interview forms are signed by all users operating within their department or area of responsibility
- Actively participate as a member of the Security Team
- Coordinate with the Security Officer on all security-related matters

Network and application administrators are technically responsible for the operation of the network or application. These administrators are responsible for assisting the departmental manager in implementing and managing information technology policies, procedures, standards, and departmental guidelines for a particular component of the operating environment. They are trained to maintain the system and must coordinate

with both departmental management and security coordinators/liasons to implement appropriate access controls for this component.

The administrators set security defaults on the system and establish the baseline control standards upon completion of a risk assessment and identification of vulnerabilities. For example, some network operating systems allow one to set the parameters for the password, such as a minimum of eight characters with at least two numeric characters. The administrators set up all security parameters and are responsible for ensuring that the users comply with these parameters. The application administrators and security coordinators work together as a check-and-balance for access control.

As stated in the beginning of this chapter, level one compliance is primarily concerned with preventative and detective controls that are monitored at this level to minimize damage to the organization. The decision to implement standards, security parameters, and monitoring tools is made at a higher level within the organization. The implementation, however, occurs at level one.

LEVEL TWO COMPLIANCE: THE AUDIT FUNCTION

The audit function is concerned with obtaining an understanding of and evaluating an organization's internal control. Internal control refers to the processes established by an organization's board of directors, management, and technical staff to provide effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. The components of internal control include:

- The control environment
- Risk assessment
- Control procedures
- Monitoring activities
- Information and communication

The integrity, ethical values, and fitness of the people within the organization establish the control environment. It is also based upon management's philosophy and method of operating, the assignment of responsibility, delegation of authority, training and development of employees, and involvement and direction from executive-level management and the board of directors. Audit seeks to ensure that the control environment is effective by assessing the stability and consistency of the factors mentioned above.

From an audit perspective, risk assessment provides identification and analysis of realistic and associated risks in achieving the organization's business objectives. The audit function seeks to establish information security controls that are proportionate to the value, sensitivity, and criticality of the systems and information being protected. This includes the probability, frequency, and severity of loss or damage that can occur.

INFORMATION SECURITY ARCHITECTURE

Control procedures ensure that management directives are implemented. Control procedures include authorization, verification, approval, reconciliation, analysis of the efficiency of operations, implementation of access controls, physical security of assets, and segregation of duties.

Monitoring activities include well-defined and scheduled management and supervisory activities to determine whether control procedures are performed effectively and consistently. It should be noted that the monitoring activities performed by audit personnel are much different from the monitoring activities performed at level one by security liaisons and administrators. Auditors monitor the control processes and procedures for indications of weakness in the control environment that has been established, while security, network, and application administrators monitor specific implementations for errors, damage, or indications of unauthorized access to systems and applications.

Information and communication in the audit environment includes the timely processing and dissemination of operational, financial, and compliance-related information to manage the business effectively.

Auditing is most often coupled with the reliability of financial reporting. This is typically so because the objective of most organizations is to make a profit. For publicly held companies, financial audits are a requirement. Within those financial audits there is a component requirement to perform computer and application reviews of systems used for critical business functions. The computer audit specialist is tasked with understanding the control and security of application systems, operating systems, networks, and databases. A large portion of these audits encompass understanding and testing logical access control to these components.

The second portion of a computer audit encompasses understanding and evaluating the general computer controls for an operating environment. Regardless of the type of hardware or software that is implemented within a computing environment, all systems have common areas of control and related control procedures known as “general computer controls.” When testing general computer controls, there are four areas of consideration:

1. Information security
2. System acquisition, development, and maintenance
3. Computer operations
4. Information systems support

Information security includes testing for logical security of online and batch access controls. System acquisition, development, and maintenance include the quality of new systems design and implementation, as well as program change control. Computer operations entail media library management, job scheduling, physical control of devices, information and data,

report distribution, backup, and recovery. Information systems support includes all of the peripherals that support an application and processing environment such as controls related to operating system software, database administration, network operations, and end-user computing.

In a financial audit, the auditors must determine what level of reliance they place on key controls. When reliance is high — which means that they trust the output data to be true and correct — a test of the key controls must be performed for completeness, accuracy, validity, and restricted access.

Controls are a combination of monitoring controls, and both manual and automated application controls. The combination of monitoring, manual, and automated controls that is tested will depend on the extent of risk and the assurance required for each control objective, the amount of coverage the control provides, the likelihood that the control will detect a problem in the application or accounting systems, and the extent of assurance provided by a particular control.

Application controls and related control objectives are procedures designed to ensure the integrity of the accounting records. Control objectives include:

1. *Completeness*: all transactions are recorded, entered into the system, and accepted for processing once and only once. All transactions input are updated to the appropriate files, and once updated remain correct and current.
2. *Accuracy*: data and information are recorded and accurately input to the computer. Changes made to data files are accurately input, and all input transactions are accepted for processing and updated to the appropriate data files.
3. *Validity*: transactions are authorized and represent true and valid transactions related to the appropriate client. Changes to existing data are not made without appropriate authorization.
4. *Restricted access*: only individuals by virtue of their job function can access data files for changes or updates. Controls protect the confidentiality of the data and physical controls protect cash and inventory.

When testing the general computer controls, the auditor is looking for potential errors in completeness, accuracy, validity, and restricted access. Tests for completeness look for controls that ensure that a given process executes in its entirety. An example of completeness for system acquisition, development, and maintenance may be that user involvement in systems design exists and helps to ensure the succession of processes through finalization. When a process completes, data, information, and audit trails are stored to be used by other processes or to be retrieved for making decisions. That this information is properly stored is called “recording.” A test of controls for recording in the area of computer operations would be to

INFORMATION SECURITY ARCHITECTURE

look at job scheduling and data library management to ensure that the proper files are being used.

Tests of validity ensure that for a process that is taking place, whether it is a calculation or allowing a user to gain access to a system, it is a relevant and legitimate process. The test performed looks at the controls over the process, not necessarily the process itself. For example, a test for validity under access control would be to determine what control exists that ensures only authorized individuals perform online approval. The control may be an organizational policy that states that only supervisors and above are allowed to perform online approval. The test would include looking at all individuals who have access for online approval and determining if all of those individuals permitted to effect online approval are supervisors and above. One notices that the test did not actually look at how the logic of online approval is applied.

Access control software is reviewed during a computer audit and includes CA-ACF2, RACF, and CA-TOP SECRET. These are software added to control access to mainframe operating systems. Databases, network operating systems, and client/server software maintain facilities inherent to the operating system itself. Software used to perform computer audits includes CA-EXAMINE, AUDITAPE, STRATA, SAS, Easytrieve, ACL, BindView, Axent ESM, Raxco Security Toolkit, OmniGuard ESM, Tripwire, and Internet Security Scanner (ISS). Internet Security Scanner can be used on TCP/IP perimeter systems such as routers, firewalls, proxy, and Web servers. These tools provide a quick and effective method of identifying security exposures as well as variances from organization policy.

Automated tools increase the depth of a review, provide a training environment to the user to better understand the inherent risks of the component being audited, and increase the efficiency of the audit if executed properly and with the proper training.

A risk-based approach to auditing determines how often a particular application or operating system is audited and will depend on the assessed risk to the organization as well as the strength of the control environment for a particular application or operating system. Information systems audits should cover the logical access path for each particular application audited, as well as general controls, which form an umbrella over some or all of the information systems in the organization. Exhibit 6-1 shows the access path from a user on a PC through the network to access an application and application data.

Controls should exist at each access point as shown to the right of Exhibit 6-1. Additionally, audits should look at the level of control throughout the entire access path. The client/server access path is different from mainframe environments. Traditionally, a single access control software

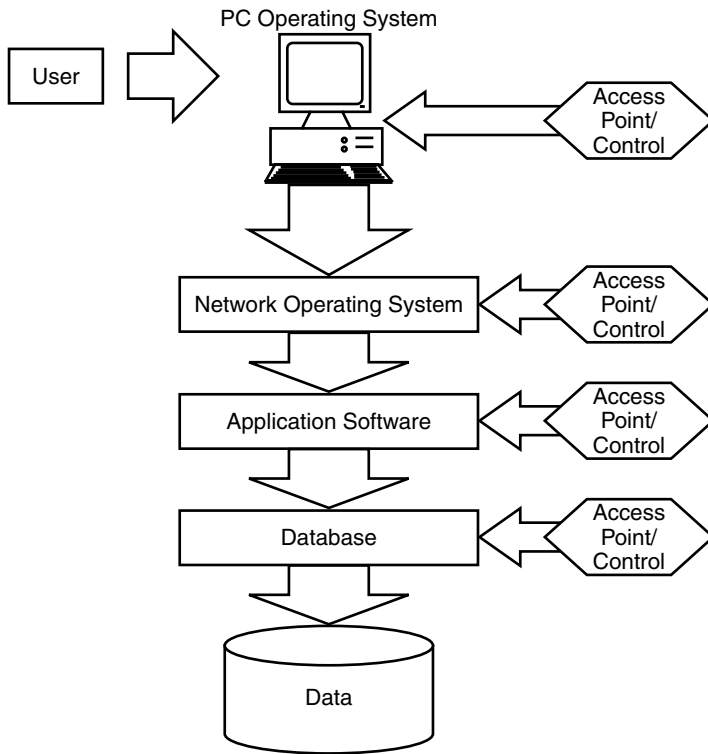


Exhibit 6-1. Client/server access path.

such as ACF2, TOP SECRET, or RACF was used to protect access to the mainframe. In the client/server environment shown in Exhibit 6-1, a separate security package can be used to control each of the access points. As shown in Exhibit 6-1, this would include four separate security mechanisms at the following points:

- PC operating system
- Network access
- Application and/or application server access
- Data/database access

Maintaining security at four levels of the client/server access path is maintenance intensive. New products are being developed to reduce the amount of administration related to security in distributed computing environments. These tools are briefly discussed in subsequent sections of this chapter.

The internal audit function should be responsible for periodically reporting on the effectiveness of information technology security policies, standards, and procedures and evaluating the appropriateness of risk

INFORMATION SECURITY ARCHITECTURE

management techniques. Another responsibility of the internal audit function is to ensure compliance with software licensing agreements. Internal audit should report their results to management and, where applicable, make recommendations for improving risk management capabilities as well as any instances where policies, procedures, and standards are not effectively implemented.

LEVEL THREE COMPLIANCE: THE SECURITY TEAM

The Security Team or Committee is responsible for ensuring that security is implemented organizationwide. An ISA provides the framework for this. Once the architecture has been defined and security policies, standards, and procedures have been established and implemented throughout the organization, maintaining security and the ISA becomes a critical priority. The Security Team is responsible for responding to technological change and for ensuring that all levels of the organization comply with the ISA.

Similar to an audit, once a security baseline of a component has been performed, a full assessment does not need to be reperformed. Only changes to the component need to be documented, along with controls related to those changes. It is similar for the ISA. An ISA that has been developed and implemented needs to be continuously assessed for effectiveness, changes to the environment that will require changes to the ISA, and modifications for improvement to the overall architecture. Compliance seeks to determine if the control objectives of the organization are being met through a consistently implemented ISA. The Security Team is responsible for the larger picture — assessing the effectiveness of the ISA.

The Security Team should not be tasked with performing audits or control testing. To use resources effectively, the Security Team will rely on the results of audits and communications with network and application administrators, as well as the departmental security liaisons, to understand the effectiveness of controls that have been implemented. The Security Team is looking for something different than that of the system auditors. The Security Team is looking for implementation of the policies, standards, and procedures that have been developed under its direction. Auditors are looking for the effectiveness of controls as they are implemented for critical programs and applications. The network administrator is concerned with the specific implementation details for a particular component.

How does the Security Team assess the effectiveness of the ISA? The Security Team should be involved in reviewing the results of all audit, control, or security reviews that occur within the organization. The Security Team is tasked with understanding why the results may not have been so spectacular and what was the systemic reason for lax or ineffective controls. The team responds to these results by assessing the policies, standards, and procedures that have been implemented and determining

whether they are realistic and can be achieved with the resources at hand. If they cannot, it is the responsibility of the Security Team to communicate to the Board of Directors or executive-level management and make them aware of the risks and attempt to obtain the necessary resources to improve the architecture.

The Security Team also acts as the investigative arm to security issues and incidences. Evaluation and valuation of a security incident will result in a change of procedure to improve detective controls as well as responsiveness. It is the Security Team that is primarily responsible for the evaluation and effecting the changes that need to take place. Incident response needs to be a clearly defined process with the objective of minimizing damage, determining the cause of the breach in security, and responding quickly to make changes to improve weaknesses and eliminate vulnerabilities. Appendix C-1 provides guidance on security incident response.

LINE OF BUSINESS (LOB) SECURITY PLAN

For large organizations that may have independent business units operating as separate companies, it is effective to have each of those business units develop a Line of Business (LOB) Security Plan. The LOB Security Plan should provide an overview of the operational environment, identify key controls within the organization, and provide the basis for measuring compliance to the corporate security policies, standards, and procedures.

The LOB Security Plan is designed to provide a baseline document for understanding the processing environment, performing baseline security assessments of that environment, and seeking to make improvements to meet the corporate goals and objectives for security. The LOB Security Plan is used as a tool for bringing awareness to each department or LOB within the organization and should become an agreement between the LOB and the Security Team to meet the defined security objectives.

The Security Team plays an integral part in assisting the LOB with development of the plan. Subsequently, it becomes the LOB's responsibility to prove compliance to corporate security policies. Changes made to the LOB's processing environment will warrant a change in the LOB Security Plan. Plans should be reviewed on an annual basis, with modifications to the environment documented and compensating controls identified and noted in the LOB Security Plan as well. A sample LOB Security Plan is shown at Appendix C-2.

ENTERPRISE MANAGEMENT TOOLS

A new generation of tools has been developed to help the organization manage the many responsibilities of providing a secure processing environment. In review, security consists of confidentiality, integrity, and availability

or continuity. Enterprise security tools are designed to ensure that assets are protected from unauthorized access (confidentiality), do not become corrupted or damaged (integrity), and that they are available for use when required (continuity). The task of ensuring that these objectives are met with the many components and multiple platforms of today's systems is a large and expensive task. Several enterprisewide tools available today include Computer Associates TNG, Axent ESM, HP Unicenter, and IBM Tivoli. These tools are designed to automate the planning, management, and control of the security policy from a single location within the organization.

One of the most difficult challenges organizations have had is not in documenting and understanding the security policies, standards, and procedures of an organization, but in implementing them consistently throughout an organization. To do so requires significant resources in man-hours. These automated enterprise security management tools are designed to offload repetitive and redundant tasks to automated processes. This is done by defining the security policy in an online database that provides the ability to test the security parameters to actual settings on each of the systems in the organization.

Reporting capabilities of the software provide tangible evidence of progress made in implementing security within the organization.

Scalability of these systems now provides the capability to centrally monitor and manage tens of thousands of systems from a single location. The same policy can be applied to a variety of different operating systems. As an example of what can be monitored and assessed, Axent ESM security modules provide the following:

1. *Account integrity*: to identify and prevent users from having security privileges that exceed the security policy
2. *Backup integrity*: to identify files that are not being backed up
3. *File access*: to examine files to verify security settings that are established in the security policy
4. *File attributes*: to identify files whose attributes have changed from the baseline
5. *File find*: to check files for viruses and other corruption that could lead to data loss
6. *Log-in parameters*: to scan for log-in parameters that fall outside the security policy
7. *Object integrity*: to identify changes in ownership and permissions for software objects
8. *Password strength*: to check the password parameters for validation against the security policy
9. *Startup files*: to examine startup files for potential security breaches
10. *System auditing*: to monitor audit trails and system accounts
11. *System mail*: to check known problem areas for security lapses

12. *System queues*: to check the security of batch queues for protection against unauthorized access
13. *User file permissions*: to check files for ownership and permissions against a baseline

The implementation of an enterprise security management system such as Axent ESM becomes a decision for executive management to make under the direction of the Security Committee. Implementations can be costly, but if managed properly provide the capabilities to provide the necessary assurance and control to all critical systems within the business.

The enterprise security management tool would be used at all three levels of compliance within the organization. Allocation of the resources for such a program would need to be approved and supported by the Board of Directors and executive-level management. Program implementation would be directed by the Security Committee and the Security Team. Day-to-day software management would be provided by network, application, and component administrators, as well as security liaisons. The reporting capabilities would be used by level one to monitor the status of system operations and security parameters. Auditors at level two could use the reports to test the effectiveness of the program's controls. Level three, the Security Team and Committee, summarizes the reports on a monthly or quarterly basis to provide tangible evidence of the effectiveness of the ISA.

There are many other tools that were mentioned previously in supporting the compliance function of an organization. Not mentioned are real-time monitoring systems that provide the capability to alert on events that indicate an intrusion could be taking place. These systems can be integrated into an organization's communications infrastructure to alert system and network administrators via e-mail and by pager when threat events are taking place. This software exists for firewalls, internal networks, routers, Internet connections, network perimeters, and applications.

Some enterprise security systems are integrating single sign-on capabilities that synchronize passwords between systems so that users provide input only once when logging on to the organization's processing environment. True single sign-on systems provide a single point of authentication for all system resources — not synchronization of passwords for multiple systems. Single sign-on provides the ability to add, modify, and delete users across platforms from a single, central point of control. When a password change is required, the password is changed across all platforms with a single modification. As the number of systems that a user must have access to increases, password management places a strain on the user.

Exhibit 6-1 revealed how a security mechanism would be needed for the user to sign on to his PC operating system. Once this was accomplished,

INFORMATION SECURITY ARCHITECTURE

the user would then have to log on to the network with another user ID and password. To obtain access to an application such as the general ledger, a user may then have to supply yet another user ID and password for the server that maintains the general ledger software as well as the general ledger application and possibly the database housing the general ledger files. Add e-mail and other application responsibilities to the user's daily activities, and just providing user IDs and passwords could waste an entire hour of productivity.

The development and maturity of security management tools is on the rise. The objective is to provide effective tools that assist the organization in maintaining appropriate and effective levels of security in a cost-effective and manageable manner. The vision is an integrated management tool that eliminates the requirement for multiple tools for each security objective.

SUMMARY

Compliance is the last step of the implementation of an ISA and of the security life cycle (assessment, design, implementation, and maintenance). Compliance is the mechanism for measuring the effectiveness of what the ISA has sought to achieve — namely, the goals and objectives of security within the organization. It is the maintenance of the ISA at a consistent and effective level to ensure that not only the security goals and objectives are met, but that the goals and objectives of the business are being met in a reduced risk environment.

The security life cycle consists of:

1. Performing security and risk assessments
2. Developing an infrastructure to reduce the risk and meet defined security goals and objectives that support the business goals and objectives
3. Implementing what has been developed
4. Measuring the effectiveness of what has been implemented, and maintaining that infrastructure to meet the needs of the organization

Having reached the final step of the security life cycle, do not stop there. One cannot stop there because in the distributed computing environment, nothing remains constant. System and network components are added daily. Employees are hired, fired, and move positions. New methods for exploiting vulnerabilities are exploited daily and must be addressed. The Internet is providing smarter, faster, and more efficient ways to offer services and do business. Nothing in the electronic world is static — and this includes the ISA. When a change is made to the operating environment, step one, assessment, of the security life cycle must be initiated. The entire environment will not need to be assessed, but that which is changed will need to be. Step two, designing controls that meet the security challenges

of these changes will have to be developed. Step three, the designed controls for those changes will need to be implemented. Once again, step four, the implemented controls will need to be tested for effectiveness and maintained. It is a continuous cycle.

The system and network administrators, security liaisons, internal and external auditors, and Security Team members are all charged with the responsibility of maintaining and measuring the effectiveness of the ISA through compliance testing. When testing results do not meet the expectations of the organization for the implementation of security, the security life cycle begins once again.

Chapter 7

Pitfalls to an Effective ISA Program

Understanding and implementing the components of the ISA is not enough to ensure a successful program. It is necessary to understand what obstacles will lie in the way of an ISA project implementation. It is very similar to studying the offensive and defensive plays of the opposing team in football, or anticipating an enemy's moves in war. If one has an idea of what the opposing team or force might do, then one is in a better position to counter their moves. The objective of the ISA is to develop a well-organized and effective security program as efficiently as possible and with minimal resistance. When one analyzes the most probable obstacles and understands how to deal with them, one will be in a better position to move the ISA project on a smooth path to completion.

There are very real pitfalls to developing an ISA. These pitfalls are discussed in this chapter so that one can anticipate them and follow through with proper analysis of the organization's environment to provide a smoother implementation. The pitfalls include:

1. Lack of project sponsorship and executive management support
2. Executive management's lack of understanding of realistic risk
3. Lack of resources
4. Impact of mergers and acquisitions on disparate systems
5. Independent operations throughout business units
6. Discord between mainframe versus distributed computing cultures
7. Corporate cultures with the objective to foster trust in the organization that contradict an environment requiring more stringent controls
8. Fortune 500 enterprises that have grown from mom-and-pop shop beginnings and do not completely support the constraints conducive to secure operations
9. Third-party and remote network management
10. The rate of change in technology

Understanding these pitfalls prior to beginning an ISA project will provide the background and knowledge to counter these issues before they manifest themselves into larger problems for the project.

LACK OF A PROJECT SPONSOR AND EXECUTIVE MANAGEMENT SUPPORT

Project sponsorship and executive management support were briefly discussed in Chapters 1, 2, and 5. This topic, however, is extremely important because it is the number one cause of ineffective security implementations and architectures and incomplete or poorly integrated security projects.

Security implementations, projects, and architectures need to be clearly understood by management so that appropriate support for the project will be provided. It is necessary to ensure that executive management understands what it is that they should be doing in terms of supporting the project. Support is provided to the ISA project when executive management has a complete and clear understanding of what the project is designed to provide and deliver. This understanding needs to include the details of project administration, scheduling, level of participation, costs, and personal and personnel commitment and constraints.

Executive management needs to be knowledgeable of all aspects of the project so that it can make appropriate decisions regarding project support. Executive management support includes an executive-level understanding of the project goals and objects, personal involvement in the project and an awareness of project status, communication throughout the organization regarding the ISA project, and approved budget for software, hardware, personnel, training, and maintenance. The ISA project workplan should be developed and presented to executive-level management so that it becomes educated on the level of effort necessary to complete a successful ISA project. Executive management will then be able to assess the workplan, ask appropriate questions to become more informed, and subsequently approve the workplan and its budget and provide communication throughout the organization regarding the project to ensure that management-level support is adequate and enforced.

Executive-Level Responsibilities

Executive management has three key responsibilities to the ISA project:

1. Understand security issues and the threat
2. Accept responsibility as ISA Project Sponsor
3. Become involved in decision-making and directing the ISA Project

Executive management can begin to understand security issues and the threat to its industry by attending security meetings and conferences and by participating in security surveys that analyze security by industry, company size, and operations. The risks are also better understood by having risk assessments performed on the networks, operating environments, and applications. Executive management should initiate these risk

assessments and remain active in the reporting and next-step planning phases of these projects.

By accepting responsibility as the ISA Project Sponsor, executive management agrees to become involved in the decision-making and to direct the activities of the ISA Project. Attending biweekly project meetings to drive the project is necessary to stay informed and provide a show of commitment to the project. Project sponsors must read and understand all project documentation, to include planning documents, status reports, and deliverables to ensure that the project remains on schedule and according to the plan, to address issues early as they are discovered, and to ensure the quality of the project deliverables.

It should be understood that it is not the sole responsibility of the Project Sponsor to figure out how to go about implementing the project or to write all of the documentation, plans, and status reports. However, it is the Project Sponsor's responsibility to understand the importance of the project, remain involved, and ensure that issues are resolved and that the project moves forward. Many project roadblocks can be addressed and eliminated with appropriate executive-level support.

EXECUTIVE MANAGEMENT'S LACK OF UNDERSTANDING OF REALISTIC RISK

When executive management does not understand the level of risk that exists, it is less likely to commit the appropriate time, energy, and financial resources to the project. Funding for security personnel, software, and security projects and programs is always more easily obtained after a major costly security incident has occurred. It is so important to not wait until a major loss has occurred, but to educate executive-level management on the risk and gain support and commitment to minimize the chance that such losses will occur — before they occur.

Executive management needs to understand security issues and the threat to its industry. Security audits and risk assessments by component spell out the vulnerabilities that exist within the organization. It is important that the results of these risk assessments are put in nontechnical terms that management can understand. Often, the results of these assessments are only communicated locally within the area or department of responsibility, such as the information systems department. The results need to be communicated to the CIO, CEO or Board of Directors, the decision makers, and those with the ability to approve funding for appropriate resources to improve the security posture of the organization.

Executive management can also be educated on security risks through a comparative study of what has occurred within the organization's industry. Security surveys are available that show incidences by industry, company

INFORMATION SECURITY ARCHITECTURE

size, and operating environment. Executives pay attention when their major competitors suffer significant embarrassment or financial loss due to a breach in security. Two industries with notable stories are banking and healthcare. Banks are concerned with wire fraud, EFT, and the Internet. Healthcare is concerned with maintaining patient confidentiality in a world where patient records, test results, and diagnoses are maintained and accessible online and more increasingly via the Internet. Executives are more likely to approve funding to ensure that what has happened to their competitors does not occur within their own organization.

Risk assessment reports should clearly state areas of weakness, the risk to the organization if the area of weakness is not addressed, and how that area of weakness can be reduced or eliminated. This allows management to make a calculated decision, either on permitting the vulnerability to remain or spending resources to minimize or reduce the risk of the vulnerability. When executive management is made aware of vulnerabilities that exist and chooses not to approve the resources to fix the problems, the responsibility of an incident then lies solely with executive management.

LACK OF RESOURCES

An ISA is a large, time-consuming, and expensive process. Projects often become derailed because of human resource and budgetary constraints. ISA projects that are initiated at the same time as large system conversions or implementations compete for the same resources. The following steps will heighten an awareness of resource constraints and allow management to prioritize and resolve issues before they negatively impact the project status.

1. Determine what other major projects are in competition with the ISA project.
2. Determine project team member commitment to the project in terms of hours per week, months on the project, and ongoing responsibilities for security programs.
3. Determine project team member commitment to other unrelated projects and job functions.

By looking at the Strategic Business Plan and the Information Technology Plan, one will gain an understanding of other projects that will draw from the organization's resources. It may be quickly assessed that the ISA project will have to be performed in phases over a longer period of time due to resource constraints. Determining this up-front will bring realistic expectations to the project rather than having to deal with the negative impact of slipped schedules and deliverables.

An analysis of the projects listed in the Strategic Business Plan and the Information Technology Plan will allow management to prioritize and allocate

funding to each project. It is very important that before this is done, that executive-level management be made aware of the importance of the ISA project and the realistic risk to the organization so that appropriate priority is placed on the ISA project.

A realistic budget for the project should be formulated. The budget should be in terms of man-hour participation, external consulting dollars, software and hardware requirements, additional security positions that will be formulated, and the cost of deliverables. Budget should be grouped into phases and by project. At a minimum, project costs should be broken down into three phases: assessment, implementation, and ongoing maintenance. Dollar allocations can then be spread over the timeframe that the expenditure will realistically be incurred.

It is necessary to take a realistic look at the obligations of the key personnel on the project. Individual roles and responsibilities should be clearly defined and an estimate calculated of hours per week that each of these project participants is required to spend on the project. Also determine the amount of time that project participants are obligated to other projects and to the performance of their primary job. Determining over-committed project personnel at the onset of the project can provide leverage in requesting external support, additional manpower, or more appropriate individual participation from someone who will be more likely to meet the project participation requirements.

THE IMPACT OF MERGERS AND ACQUISITIONS ON DISPARATE SYSTEMS

In today's world, mergers and acquisitions are all too frequent in every industry. A merger between organizations often results in the acquisition of multiple and differing sales, inventory, financial and accounting programs, and the systems and hardware on which they run. The merged organizations may also use differing security tools, programs, and compliance testing procedures. Decisions must then be made to convert to a single application, eliminate disparate hardware, maintain both sets of systems, or converge packages and systems into a hybrid. In some acquisitions, equipment and computing systems may be sold. On the other hand, a requirement may exist to maintain older systems to be able to continue to access sales and financial records. These decisions will have an impact on the resources used for security.

In any merger and acquisition, there will be security implications. Security personnel will have to learn and understand the new systems in order to maintain them. Security initiatives will have to be developed for the acquired set of applications and systems. There may be a requirement to perform security assessments to ensure that the acquired networks, systems, and applications are in compliance with the security policies and procedures of the parent organization.

INFORMATION SECURITY ARCHITECTURE

For larger organizations where information systems departments exist in both of the merging organizations, the decision will have to be made to either eliminate one department, combine departments, or continue to maintain two totally separate departments. The decision to eliminate one department and convert to a single set of applications and systems will have the least impact on security in the long run because there will be fewer systems to maintain. The decision to develop a hybrid or maintain disparate systems creates an increased burden on security personnel, who will have an increase in the number of systems that need to be assessed and monitored for compliance.

Eliminating one department usually indicates that the existing security policies, standards, and procedures of the dominant organization will remain in effect. Combining departments may require a rewrite of the policies, standards, and procedures, taking best practices from each organization and creating a better set of methods. When the decision is made to continue with both information systems organizations, allowing them to operate independently with their own management, personnel, and equipment, some security issues will definitely arise. This is discussed in more detail in the section on Independent Operations Throughout Business Units.

Often, mergers and acquisitions result in the acquired organization continuing on with its own management structure, departments, systems, and personnel as if it were a separate department or business. In this situation, both organizations may operate under their own policies, standards, and procedures. For security, however, it may be necessary for the parent or dominant organization's corporate policies and standards for security to be adopted by the acquired organization. The burden of proof for compliance to security policies and standards should remain with the dominant or parent security department to ensure that the newly acquired systems and programs are in compliance. When both organizations are operating independently with their own executives, budgets, and financial statements, it may become very difficult to force one set of security policies, standards, and procedures on the acquired organization. The policies and standards may require the newly acquired organization to purchase, install, and maintain expensive hardware and software to test security compliance. Also, annual security reviews or audits may be required. An issue or problem begins to occur when the acquired organization is also forced to bear the burden of the cost for security equipment, software, personnel, and dollars to support the policies and standards.

This situation requires good communication between the two merging organization's security counterparts. It also requires a certain amount of give-and-take. The dominant organization may want to absorb some of the cost for new security equipment and software that the acquired organization is required to obtain to be in compliance with existing programs. The

dominant organization may want to offer security consulting and assistance to the acquired company to provide quick-hit improvements. In any case, executive-level support will be key to resolving the problems created by mergers and acquisitions.

There is particular concern regarding opening a connection between the networks of the merged organization. Initially, it will almost always be the case that one of the organizations has a weaker security program than the other. Connecting the networks would increase the exposure to the organization with tighter security. Before a connection between the two organizations is established, it is necessary to understand the security posture of both organizations and bring them to comparable levels before opening this bridge. Firewalls can be established to ensure that the risks and exposures are minimized between organizations.

The impact that a merger or acquisition will have on security can be managed. The security organization needs to be brought into the planning process for the merger or acquisition. Security information regarding the new organization should be gathered prior to the merger decision. The impact on security should be analyzed and communicated to executive management so that it is aware of the security implications. The following information should be gathered for impact analysis:

- Inventory of applications, operating systems, and hardware
- Type of e-mail and voicemail systems
- Type of network operating systems
- Number of network nodes and network diagrams
- Interconnectivity between metropolitan and remote locations
- Firewalls and Internet connectivity
- Security policies, standards, and procedures
- Number of individuals dedicated to security
- Organization chart and the roles and responsibilities dedicated to management of the above equipment
- Virus scanning software used
- Security compliance software used
- Documentation of security assessments

This information will be used much like a security audit or review. A high-level assessment will give the Security Officer the ability to understand the depth of security within the acquired organization. An assessment of the applications and systems will indicate the amount of disparity between the two organizations. The Security Officer should properly educate executive management on the impact that the merger will have from a security perspective. The Security Officer is responsible for making recommendations to management regarding maintaining a secure environment during the transition of applications, systems, and networks. Although the Security Officer is not typically the individual who makes the

INFORMATION SECURITY ARCHITECTURE

decision regarding which systems will be kept, converted, or eliminated, these decisions must be communicated to the Security Officer so that he can make appropriate decisions regarding implementation of security in the reorganized environment.

INDEPENDENT OPERATIONS THROUGHOUT BUSINESS UNITS

Some organizations maintain independence throughout their business units (BUs). Each BU may have its own company name, its own CEO, CIO, and CFO, or maintain its own human resources, information systems, and security departments. This independence may be necessary by virtue of the different services offered or products developed by each BU. Independence may also be granted to a BU that is the result of a merger or acquisition. Independence may also be a result of the mere size of the organization. Independence here means that the management of each BU is free to run its BU according to its own management style, decision-making entities, and internal policies, standards, and procedures. The BU is free to select its own hardware, operating systems, applications, e-mail, voice-mail, and security tools and processes.

This way of operating is common in many industries and will have a certain impact on the implementation of security. An example of the issues that will arise through independent operations can best be described from a consulting engagement to consolidate help desk support for a state government. Each of the individual departments — Department of Agriculture, Department of Health, Department of Internal Affairs, etc. — was given the ability to run the department as it saw fit. Each department offered very different services and required very different processes; however, they did report to a centralized management structure. Each department purchased its own applications, PCs, e-mail, voicemail, and ran its own information systems department. As the need for communication between departments increased, the state began to realize the inefficiency of running 11 different IS departments, having a handful of different e-mail, voicemail, and network operating systems and, running 11 different IS organizations with 11 different help desks. The state was having great difficulty communicating between departments and spending an even greater amount of money on redundant tasks within each department.

While granting the ability to operate independently appears to be a benefit to those responsible for managing the BU, it can hinder the efficiency, interoperability, and communication between BUs. Its effect on security is also a significant concern. Interconnecting 11 different BUs with 11 different standards for security allows for an extremely insecure environment. It also requires more tools and work programs to handle the increased amount of nonstandardized equipment, software, and programs. Security and independent operations as described in this chapter is not particularly harmonic.

The argument should be made to the BU for centralizing the management structure of security in the decentralized or independent operating environment. Decentralization in this case is pushing the majority of operations and decisions down to the department or BU level. Centralizing the management structure of security for the BUs described in this study is extremely difficult but can be achieved. First, one must argue the case for a centralized management structure for security. Cost, efficiency, and standardization are the greatest arguments. The parent organization is ultimately responsible to ensure that each of its BUs remains profitable and sound. Security policies that apply to all BUs within an organization and make security consistent across BUs will achieve the goal of standardization. Maintaining a standard set of tools and procedures for security will lessen the cost of each department maintaining its own set, and will provide efficiency in having a single body of knowledge to pool from regarding the standard set of tools.

Politics in security will be necessary because each of the autonomous department or BU heads will not want to be told how security is to play out in their organization. Again, the first step is to demonstrate the risks and importance of security. The second step is to give the BU alternatives in implementing security. For example, BU management can implement its own tools but must demonstrate compliance to corporate security policy on an annual basis. If the BU maintains its own set of tools, it would then have to develop a reporting procedure that demonstrates compliance to each point in the security policy. The other alternative the BU can be given is to use a set of standard tools and procedures provided by the parent organization. If the BU chooses the standard set, it would not have to develop a compliance mechanism because the parent organization already has one designed for the standard set of tools.

Often, giving a BU the opportunity to make its own decisions regarding security will make its management more receptive to the goals and objectives of the overall security program. Demonstrate to the BU the benefit of taking away the burden of security from the BU. The parent or corporate organization should be willing to bear some of the costs of administration, and this cost burden should be presented to BU management as well. It is necessary to demonstrate to the BU the:

- Importance of security
- Liability to the organization for any incident that occurs
- Necessary and appropriate controls to minimize risk
- Requirement to demonstrate compliance to corporate security policies
- Cost benefit of centralizing the security management structure
- Consulting and assistance available from the corporate security personnel

INFORMATION SECURITY ARCHITECTURE

Educating, reassuring, and assisting BU management with security program initiatives without forcing security decisions on them will foster a better working environment for security and help to maintain the goals of a cost-effective, efficient, and standardized security program.

DISCORD BETWEEN MAINFRAME VERSUS DISTRIBUTED COMPUTING CULTURES

The Executive Summary of this book pointed out that ten to fifteen years ago, the majority of businesses operated closed processing environments. Processing platforms were proprietary, typically located in one central site and, more than likely, within a single room. Data input to the mainframe was via terminals that provided one-way communication. Computer rooms were restricted to a handful of individuals and were behind big glass windows often referred to as “glass house.”

The “glass house” provided limited and controlled access to information and sensitive processing programs and resources. The move to distributed computing brought greater empowerment and increased efficiency to the users, but opened up a multitude of control issues that need to be considered and addressed when moving to this type of processing environment. In the days of centralized processing and mainframes, information security was the responsibility of one individual, the mainframe security officer. Now, information security touches everyone within the organization and requires significantly more personnel involvement, commitment, and management.

For organizations that have made the transition from mainframe to distributed environments, existing management and staff trained in the mainframe environment have had to choose between retooling for the distributed environment or moving on to other endeavors. Some organizations invest in retraining their processing personnel. Others have attempted to make the transition without providing appropriate training for their staff, expecting that the existing staff will pick up the necessary skills from on-the-job training. And still other organizations have added to their staffs by hiring individuals with the necessary distributed processing skills.

For those organizations that have not invested in training for their staff and expect existing mainframe personnel to implement the appropriate control structure, it is typical to see what can be described as the “round peg in the square hole.” IS departments take policies, standards, and procedures related to controls in the mainframe environment and modify them slightly, substituting references to the mainframe with distributed processing. Their attempt is to rewrite those same documents to apply to the distributed environment.

Mainframe personnel are often concerned with the stability of their position in the company. They may make every effort to conform to and

educate themselves about the new environment; however, their primary training lies in mainframe processing. The threat is that newly trained individuals are replacing their expertise and them. There may be some resistance to the new staff, the new environment, and the requirement for more stringent controls. Selling an ISA and a more comprehensive security program to a shop run by a mainframe manager can be difficult.

To remedy this, the education process must include communication, with the mainframe staff gaining its buy-in and promoting its understanding of the necessity of an ISA. It is important to help the mainframe staff understand what its role can be in the ISA. It is also important to obtain the necessary resources from management to retool the mainframe staff. Until the current mainframe staff is educated on appropriate risks and controls of open network environments, much vulnerability will continue to exist during the transition from mainframe to distributed processing.

When an organization maintains both a mainframe and a distributed environment, it is also necessary to ensure that the appropriate management structure is in place for the redefined organization. Placing legacy mainframe management over distributed computing personnel may not be effective or appropriate. It is necessary to ensure that the management responsible for the distributed environment is appropriately knowledgeable of the risks, controls, and operations. It is also necessary to ensure that the management of this new environment does not have a vested interest in keeping things the way they were, not the way they should be. As the environment grows to accommodate both environments, so should the management structure. Management personnel responsible for both environments but with an expertise only in mainframe processing will tend to pay more attention to what they know rather than what they do not know and do not understand.

It is recommended that the changes made to the processing environment over the past ten years be reviewed, along with the management structure that supports it. If there have been significant changes in hardware, operating systems, and applications but the number of individuals supporting those changes have not increased or the positions are supported by the same people over the past decade, it may be necessary for a manpower review. This would entail an analysis of each position, its job description, functions and tasks, educational requirements, average workday statistics, overtime, and wage increases. Many IS departments function with overworked, underpaid, or undereducated personnel who are not able to perform the necessary tasks to create an effective, efficient, and secure processing environment. This can be a result of the fact that they are either not capable, not willing, or do not understand what is required.

FOSTERING TRUST IN THE ORGANIZATION

Many organizations desire to establish a feeling of care and trust within the work environment and as a part of their corporate culture. Management within these organizations has indicated that implementing stringent security controls would contradict these initiatives of fostering trust. Security policies that spell out consequences are viewed as a threat. Restricting access times, changing passwords, and limiting concurrent log-ins impede operations and only serve to agitate employees and promote suspicion.

While these arguments have some merit, does that merit outweigh the financial and operational risk to the organization? Management must look at the consequences of having less stringent controls. Will fostering trust be as important to the organization when an incident occurs that has caused a significant financial loss or quite possibly has affected the reputation of the company? The answer is, probably not. In such instances, the company may place a priority on security but can also maintain a priority on the objective to foster trust. It is not necessary, however, to pick one over the other. In such cases or arguments, one can be more sensitive in how one promotes security in such organizations while maintaining a secure environment at the same time.

In all organizations, it is necessary to take a look at the corporate culture and define ways to meet security objectives while keeping in mind how the organization operates. It is necessary to understand the philosophies and psychology of the organization, its management, and its employees to be able to more effectively promote security. Questions that may provide some of this background are:

1. How is the relationship viewed between management and staff?
2. What type of voice do the employees have in promoting or improving operations?
3. Are the employees shareholders?
4. Do the employees benefit by increased sales and profits?

Look at questions #1 and #2: How is the relationship viewed between management and staff? What type of voice do the employees have in promoting or improving operations? Analyzing the answer to these two questions will indicate whether management dictates rules and regulations that must be followed by all employees, or if management places a lot of responsibility and decision-making ability down at lower levels throughout the organization. This may indicate at what levels within the organization one will need to gain buy-in. If management operates in an autocratic or dictatorial manner, then what management says probably goes and it is most likely not publicly questioned very often. However, if decision-making is made by supervisors and managers within each department, then it will be necessary to treat these decision makers with due respect and “sell” the project or gain buy-in to them as well.

Take a look at questions #3 and #4: Are the employees shareholders? Do the employees benefit by increased sales and profits? A positive answer to both of these questions indicates that employees share ownership and responsibility for the organization. As an employee with stated ownership, it is the responsibility of management to ensure that all employees understand the risks to the organization of which they are part owners. Whether or not they are part owners, all employees inherently benefit from increased sales and profits through some degree of job security, and all employees should be educated on risks and benefits.

More stringent controls will not deter a feeling of care and trust within an organization. It is how and what is presented to the employees that could possibly affect the corporate culture. If the ISA or components of it are presented in such a way to indicate concern for the organization's stability, profitability, and ongoing welfare, each and every employee will understand the necessity and importance of this significant program.

MOM-AND-POP SHOP BEGINNINGS

Some of the more popular Fortune 500 enterprises have grown from Mom-and-Pop shop beginnings and sometimes do not completely support the constraints conducive to secure operations. There are two reasons for this: trust, as explained in the previous paragraphs, and the way business has always been done.

It was once explained to this author by the CIO of a Fortune 500 company that they had begun their business in a garage (much like Hewlett-Packard). The majority of the employees had lived within several blocks of the plant for most of their lives. Many of the employees were friends, neighbors, or relatives. There was not one employee who this CIO did not know or trust. This company manufactured internationally recognized cookware and maintained retail space in such stores as Macy's, Kaufmann's, JCPenney, and Lazarus. What prompted this conversation was the discovery that the system defaults on the main processor's operating system software had not been changed from the defaults that had been shipped with the software two years prior. There were guest accounts and the password for the sysadmin account was sysadmin. Essentially, the entire accounting, inventory, and sales information was accessible to anyone; there were no regular backups being performed; and there were no contingency plans available.

Companies such as this one, whose sudden growth surpasses the company's ability to scale the necessary operational and management structure to meet that growth, often do not realize the impact to the business if their operations were to suddenly stop. In this case, it was explained to the CIO that any sudden inability to stock products in retail stores would result in loss of shelf space in those stores.

The other argument that is given in this scenario is that “this is the way business has always been done.” Management has a resistance to that which it is not sure of. Many executives were averse to having a PC on their desk, voicemail, e-mail, and the Internet. Now, these same CEOs have found that they cannot remain competitive without these technological capabilities. Running a garage shop and stocking shelves in nationally and internationally known retail stores are two very different realms. Operations that hang onto the “this is the way business has always been done” attitude are probably not long for this world. One can only imagine what has happened to some of the CEOs and their companies that had maintained this attitude at the advent of computers.

Again, the executive management, supervisors, staff, and employees must all be educated on the realistic threat of today’s computer-driven operational environment. An understanding of the threats and risks, security, its purpose and appropriate implementation are the first step in leveling the resistance from organizations that have grown so rapidly. Trust and the Mom-and-Pop shop familiarity can continue to be present as a part of the organization’s culture, but the open operating environment must change to meet the risks and threats of today’s networked processing environment. Management must shift its thinking to encompass the reality of doing business in today’s electronic and open world.

THIRD-PARTY AND REMOTE NETWORK MANAGEMENT

Many organizations outsource their network operations because they do not want the added staff or they do not have the personnel trained to manage their networks internally. Maintaining a secure environment in outsourced or remotely managed network operations can be difficult if the outsourcing contract is not appropriately managed internally.

There are several things to consider in outsourcing and remote network management. When network management is outsourced, often the transmission path of company data and information is shared by other organizations as well. The company’s data may be multiplexed with another company’s information while traveling through the same transmission pipe or channel. It is necessary to ensure that sensitive information is protected through a mechanism such as encryption. This is true for all shared networks — not just organizations that outsource their network management.

Typically, outsourced personnel are managing not just your network but other organizations’ networks as well and will develop procedures conducive to doing their job more easily, not necessarily making your organization’s network secure. For example, a major steel company had outsourced its network operations. It was discovered through an audit that the outsourcer was setting up access to each of its client’s hardware and software, including routers, using the company name as the user ID and the company

name also as the password. The outsourcer was doing this for both the outsourcer's internal management software and for access to software and hardware owned by the client. This made it easy for the outsourcer to manage several different clients. It was not, however, at all secure for the contracting organization.

Inevitably, if security is not a priority when the outsourcing contract is written and the contract does not include necessary and specific procedures to audit and ensure compliance with the organization's own security policies, standards, and procedures, then security will definitely not be a priority with the outsourced agent. Security will only be as strict as an organization demands in a contract and on a measurable basis. If network operations are outsourced, an organization's internal security personnel must be knowledgeable of the procedures related to network access and modifications to the network architecture. Security personnel should be involved in any contracts related to the outsourcing. Procedures must be developed that allow the organization to monitor and audit the outsourced contractor's performance. If security was not considered prior to signing a contractual agreement, it is usually very difficult to amend the contract for security after the fact.

Network management contracts are binding and can also technologically impair an organization. One of the largest public networks in the United States held one of the largest credit card companies virtually hostage with their network management agreement. This credit card company was completely revamping its LAN, applications, and distributed processing environment. The capacity needed for the LAN to run these applications was significantly more than the original network design. The network management vendor would not upgrade the network or install routers with more capability and capacity under the current contract which was valid for the next several years.

In this same example, the contracting organization did not have the ability to view its own router configurations online. It had to request a meeting, which took several weeks to schedule, to review configurations and changes to its own network. As suggested in the previous paragraph, it is necessary to build into the network management contract, the ability to audit and monitor the performance of the outsourcer. It is recommended that designated internal personnel be able to view the network configurations, access, and changes that are made to its own network. Many outsourcers do not permit the contracting organization to have any access to this type of information. Most outsourcers argue that they are fully responsible for its configuration and do not want interference from the contracting organization. To an extent this is true. Very few individuals should have the capability to access and modify the existing network. However, the contracting organization should have the ability to read-only access to view such things as log-in

INFORMATION SECURITY ARCHITECTURE

IDs, network operating system access lists, router access control lists, fire-wall configurations, and security-related default settings.

The contracting organization and the outsourcer should work together in a series of checks and balances when it comes to network security. When an external connection or access is permitted for a contractor, consultant, or outsourced entity, it is wise to have each connection require a new password that is provided to the contractor from an contracting organization. Once the work is complete or the workday comes to an end, the password is changed and any further access would require a request for a new password after proper validation of the external entity's identity. This allows for an audit trail of access from outside entities and minimizes their unlimited access. However, getting away from this type of day-to-day internal management may be one of the reasons that outsourcing was considered in the first place. If the outsourced network management entity needs continual access, then it is appropriate to establish the guidelines for the outsourced entity to follow. An example might be:

The network management entity will establish user IDs according to Starcross policy. All user IDs will consist of the first four characters of the user's last name and the four-digit numeric code that establishes the user's status within the organization.

The network management entity will establish passwords for all external connections and access to Starcross proprietary software that meets the standards of internal Starcross Security Policy. Passwords will be a minimum of eight characters in length with a combination of alpha and numeric characters. These passwords will be changed every 30 days. Network management company employees will not share passwords. Each individual responsible for managing Starcross networks will have a unique user ID and password...etc.

When outsourcing network management and operations, internal technical expertise should assist in the establishment of the contract. If internal expertise is not available, it would be wise to have an external consultant knowledgeable in network security to assist in the development of the contract and to ensure measurable procedures are developed for both auditing the network manager's performance as well as ensuring compliance to internal security policy. The contract should specify — at a minimum — the following:

- Requirement to sign and accept internal confidentiality agreements
- Accepting and abiding by the contracting organization's security policies and standards
- Set up of user IDs
- Minimum password length
- Password change parameters
- Validation and authentication of users

- Network management tools
- Network monitoring requirements, tools, and procedures
- Intrusion detection requirements, tools, and procedures
- Acknowledgment and notification of external account managers
- Points of contact and notification procedures
- Emergency response and escalation procedures
- Problem resolution
- Required timelines for response and problem resolution
- Disaster recovery and continuity of network operations
- Ability of the contracting organization to view online (read-only) network and router access and configurations
- Change control procedures
- Network performance requirements and statistics
- Modifications to the contract

Penalties may also be established against the network manager for breaches in security. This will provide an incentive to operate the network environment in a most secure manner. The list above is not an all-inclusive list of items to consider in the network management contract. Network security and management procedures should be reviewed with an objective network manager, either internal or contracted, to understand the full scope of what should be defined and documented in the outsourcing contract.

Remote network management also presents some security challenges to the organization. Remote network management may be performed by an outsourced entity or internally to the organization. On most occasions, outsourced network management is performed remotely. Essentially, being able to remotely access and manage a network means that other potentially undesirable and unauthorized individuals can also access the network and the remote management capabilities.

The most desirable and secure method of management is to require logging on to the network operating system from the local console containing the management software and restricting remote access to that console. This applies to routers as well, restricting access and modification to the routers only from the local console. Unfortunately, today's networks can stretch from city to city, across the country, and even internationally. Flying a certified network manager to the location of the hardware and operating systems or having certified individuals at each network location can be unreasonable and costly. Remote network management is employed because of distance, personnel, and operational constraints.

It is important that when remote network management is employed, the security controls related to accessing the management functions be most stringent and frequently monitored. Access should be limited to a very small number of qualified personnel. Passwords should be changed much more frequently, such as on a weekly basis. Audit logs should be active and

reviewed by qualified individuals. Authorized and unauthorized users who gain access to sensitive network management functions have the ability to shut down the entire distributed operations.

Remote and outsourced network management is presented in this chapter because their employment places a burden on the management of security. It is very difficult to dictate to someone outside the organization how they will proceed and what priority they will place on security. Loyalty to the organization is more difficult to instill in someone who is not a true member of the organization. Security is only a piece of the network manager's responsibility. Many network managers work long hours beyond the eight-hour day and are on-call 24 hours a day to handle issues and emergencies. Security is often overlooked or never quite made a priority. It is necessary to clearly define the security requirements through appropriate and complete documentation and within the confines of the outsourcing contract. It is also necessary to make security requirements more stringent for those who hold the keys to the operational kingdom.

THE RATE OF CHANGE IN TECHNOLOGY

The final "pitfall" discussed in this chapter is the rate of change in technology. As witnessed over the past decade, technology changes so quickly and that rate of change seems to increase as time goes by. Software version upgrades come to market at a faster rate. New strains of computer viruses are introduced on almost a weekly basis. From e-mail to voicemail to DVD, information systems personnel are inundated with choices of applications, hardware, available tools, and which technologies will provide the greatest competitive advantage.

The rate of change in technology also provides a challenge to the security manager. As more technologies are employed, there becomes a requirement to secure that investment. Security personnel must learn about each and every hardware device, operating system, software application, and access device to ensure that they make the best and most cost-effective security decision related to that device and for the organization's operational benefit. They must also prioritize where the greatest risks are and how security resources will be used most effectively.

Five years ago, security tools were young to the market. Some of the most popular software was freeware downloaded from the Internet that was used to scan and test operating systems. Vendors have taken versions of that freeware and provided much more functionality and significant capabilities at a much greater cost. Security tools are now extremely competitive and the number of companies dedicated to providing security software and consulting is growing at a fast pace. The one catch is that security products that are popular, effective, and highly touted in today's

operating environment, may become a product surpassed by its competitor in future releases.

The cost of security is increasing. Continuous network monitoring requires FTEs. Internet access requires firewalls and personnel to manage those firewalls. Each new product and upgrade requires an evaluation of the functionality, capabilities, vulnerabilities, and risks. As operating system and software upgrades are released, hackers are diligently working to find the weaknesses and loopholes. The dynamic nature of the distributed processing environment deems it necessary to always be evaluating, monitoring, upgrading, and researching — which can become a burden to the security professional.

The greatest pitfall in security is to assume that security is static: that once a security tool or program is in place, it will perform its function on its own. Many companies have made this mistake in relation to firewalls. Firewalls must be monitored for access attempts and analyzed for the types of traffic that are transversing its ports. A firewall must be periodically tested to ensure that its configuration is sound and is meeting the operational and security requirements of the organization.

Never become complacent in regard to security. What is secure today may be full of loopholes tomorrow. Security, like technology, is extremely dynamic. It is prudent to provide security personnel with the time necessary to perform research; read professional journals, magazines, and periodicals; attend security conferences to learn of the most recent vulnerabilities; and make educated decisions regarding the best products. This responsibility should be included in their list of job functions and documented with their job description. It is also good to join peer groups that discuss best practices and sponsor vendor demonstrations.

A final recommendation is to expend the necessary budget to appropriately train security personnel on the tools that have been chosen to protect the organization. Many, very expensive security tools have been installed and then ignored or have sat on the shelf because trained personnel were not available to use them. Training and conferences should be automatically included in the annual budget so that security personnel can plan and prioritize their greatest needs. Following these recommendations will allow security personnel to remain informed and better able to make sound business decisions related to security.

SUMMARY

This chapter is designed to make the reader aware of the pitfalls that exist and that can slow the progress of an ISA project. Understanding how each of these issues could negatively impact security within the organization will help one manage the issues before they become problems. Decision

INFORMATION SECURITY ARCHITECTURE

makers will find many reasons not to pursue an expensive ISA project that, if misunderstood, appears to have a small return on investment.

The first pitfall is a lack of understanding of the very real threats, vulnerabilities, and risks that exist in today's operating environment. Appropriate education of executive management, supervisory staff, and employees will help to gain buy-in and support for the ISA project. A high-level project sponsor must be appointed and must understand his roles and responsibilities so that he can continue to drive the momentum of the security program.

The necessary human and financial resources required to initiate, implement, and maintain a security program must be clearly defined in a project plan and prior to project initiation. Many projects get started and fall short of completion because the required personnel or dollars are not available to continue with the project. A long-term view of realistic costs helps to communicate the necessary commitment to an effective program. Surprising the decision makers about financial requirements in the midst of an ISA already initiated tends to cause ill will and dwindling support because resources must then be diverted from other projects.

Corporate culture and management style are two very important factors that must be researched and understood. Presentation of the implementation of security will depend on the goals, objectives, and management styles of those in charge of the organization. Giving each department autonomy in how it chooses to run its operations will impact how and to whom the ISA project is communicated. It will also affect standardization of policies, procedures, tools, and equipment throughout the departments or business units. The goal to promote trust within an organization may cause resistance to the ISA. Tightening security controls may be perceived as a lack of trust toward the employees or an expectation that something is bound to go wrong.

Mergers and acquisitions will affect the necessary resources for security. New and different equipment and systems will require skill sets necessary to manage the security of that equipment. Security personnel should be involved early in the planning stage for mergers and acquisitions.

Processing environments have changed so quickly that it is difficult for security personnel to stay abreast of each new vulnerability and the available tools. Management must be sensitive to the need for educating its personnel who are skilled only on legacy systems that may become obsolete. Employees who fear their jobs are not secure due to the rapid change in technology may demonstrate resistance to changes in the operational environment. Technology and vulnerabilities change so quickly that constant education and research is necessary to be effective.

Knowing what makes large projects fail and understanding how to deal with the resistance, constraints, and arguments will help to keep the ISA project on track and viewed as a positive and successful initiative.

GETTING STARTED

The following steps will help ensure success and support of security in an organization.

1. Ensure there is a project sponsor who understands his role and responsibilities in the ISA project.
2. Educate executive management so that it understands the risks to the organization and is aware of the level of support needed to be dedicated to security and the ISA project.
3. Define a project plan that includes a budget and long-term planning for personnel and financial requirements to effectively move the ISA project forward.
4. Have security personnel involved in the initial phases of information-gathering and decision-making for mergers and acquisitions to ensure effective communication of the impact to support security and ensure the proper disposition of systems and equipment.
5. Encourage the standardization of security policies, procedures, and tool sets within organizations that promote independent operations of their departments and business units.
6. Understand the need to provide cross-training to employees responsible for legacy systems. Supplement mainframe staff with fresh personnel trained in the distributed environment who may better understand the risks, vulnerabilities, and control requirements of that environment.
7. Research and understand the management style and culture of the organization. Present security in a nonthreatening manner, with the main objective to protect the organization's financial and operational stability.
8. Involve trained personnel in the establishment of third-party and outsourced network management contracts to ensure that internal personnel have enough leverage to enforce internal security policies and can monitor compliance effectively.
9. Stay abreast of changes in technology. Attend seminars, read journals, and confer with industry peers in order to make suitable, long-term, and cost-effective decisions related to security.

Chapter 8

Computer Incident / Emergency Response

Introduction

This chapter discusses the general concepts involved in incident response handling. This includes the development and management of a Computer Security Incident Response Team (CSIRT) or Computer Emergency Response Team (CERT®) and its day-to-day operations. CSIRT operations include recognizing events and incidences as they are occurring, examining what has been reported, gathering as much information as quickly as possible, applying known solutions to an intrusion, stabilizing the system, and performing objective analysis of the incident to ensure thorough response, documentation, and to provide lessons learned. The faster and more organized an enterprise is in reacting to an incident, the less damage that will be caused by that incident. Rapid response with known reactive procedures can help prevent incidents in the future. Mature CSIRTs can also provide preventive measures that help to minimize the risk of events and incidences and decrease the number of occurrences.

Learning Objectives

When finished reading this chapter, one should be able to:

- Understand the general concepts involved in the day-to-day operation of a CSIRT.
- Understand the three phases of CSIRT as defined by the CERT/CC.
- Understand the four phases of CSIRT as defined by the Army CERT (ACERT).
- Understand the classification of an incident.
- Identify key organizations that provide CSIRT operations.
- Understand the requirements of developing a CSIRT.
- Identify issues and steps in forming a CSIRT.
- Define these acronyms related to a CSIRT:
 - Army Computer Emergency Response Team (ACERT)
 - Automated Information System (AIS)
 - Computer Emergency Response Team (CERT®)
 - Computer Security Incident Response Team (CSIRT)
 - Computer Incident Response Team (CIRT)
 - Incident Response Handling (IRH)

INFORMATION SECURITY ARCHITECTURE

- Define these key terms related to incident response handling:
 - Artifact
 - Chain of custody
 - Constituency
 - Containment
 - Eradication
 - Event
 - Forensics
 - Incident
 - Identification
 - Intrusion
 - Proactive
 - Reactive
 - Recovery
 - Tracing
 - Tracking
 - Triage
 - Vulnerability

Previous chapters emphasized the dependence that organizations now have on their networks and computer systems. Networks and the Internet have made the technology infrastructure more vulnerable to attacks with an increase in the number of computer security incidences. Additionally, the complexity of the technology infrastructure has made it difficult to manage the administration of this infrastructure with limited resources. Having appropriate security policies, standards, and procedures; performing security baselines of components; and designing and implementing secure configurations for the components of the technology infrastructure contribute to reducing the risks and vulnerabilities. Despite a solid and effective ISA, there is no guarantee that computer incidences will not occur, and the organization must be prepared to respond quickly and effectively to minimize damage and loss. The Computer Security Incident Response Team (CSIRT) is a group designed to respond to such occurrences in a formalized manner and is the topic of this chapter.

CSIRTs are being developed within organizations to respond to the increase in computer incidences. CSIRTs are the means necessary to formalize incident response methodologies, processes, and organizational structures. This includes formalizing and standardizing a process for notification, communication, collaboration, coordination, analysis, and response. These methods, processes, and structures are still relatively new to the ISA and are considered in the infancy stage of the security life cycle. No standards have been set for incident response handling (IRH) and CSIRTs although efforts are ongoing to develop those standards. For this reason, it is necessary to look at the specific requirements of the organization and its

risks to determine the placement, size, operational capability, and services offered by the CSIRT.

CERT®/CC

CERT® is an acronym for the Computer Emergency Response Team and originated at Carnegie Mellon University (CMU) in 1988 to address the Internet security concerns of the research community. The name was changed to The CERT® Coordination Center with the acronym CERT/CC and is now part of the Software Engineering Institute at CMU. Although CERT is often referred to in a generic sense, like the word “Band-Aid,” CERT is registered in the U.S. Patent & Trademark Office for CMU just as “Band-Aid” is a registered trademark of Johnson & Johnson.

The CERT/CC is recognized as the foremost leader in incident and emergency response because of its history, charter, and years of experience on the topic of network and computer incidents. The CERT/CC offers online advice and whitepapers on the subject, methodologies, research, as well as classes and certifications. The CERT/CC is a formal and cooperative organization designed specifically to deal with incidences. The CERT/CC developed the term “CSIRT” (or Computer Security Incident Response Team) as the generic term that can be used by organizations in developing an organizational group that responds to computer incidences and emergencies.

There are other terms in addition to CERT and CSIRT that are used to describe computer incident response teams. These terms have not been registered as trademarks and can be used in the development of your organization’s response capability. They include:¹

- *CIRC*: Computer Incident Response Capability
- *CIRT*: Computer Incident Response Team
- *CSIRC*: Computer Security Incident Response Capability
- *IHT*: Incidence Handling Team
- *IRC*: Incident Response Center / Incident Response Capability
- *IRT*: Incident Response Team
- *SERT*: Security Emergency Response Team
- *SIRT*: Security Incident Response Team

To ensure no infringement on the CERT trademark, we refer to this group as CSIRT throughout this chapter. CERT, however, can be used by other organizations but only with written permission from the CERT/CC. This can be done via e-mail to cert@cert.org.

CSIRT Goals and Responsibilities

The goal of a CSIRT will differ from organization to organization. The goal of the CSIRT must be based on the business goals and objectives of the

organization. The goal of both the business and the CSIRT will include protecting critical assets within the organization. In doing so, the CSIRT is designed to “minimize and control damage, provide effective response and recovery, and work to prevent future events from happening.”²

The responsibilities of the CSIRT will vary, depending on the structure of the security organization in an enterprise and the amount of resources available to establish this team. The team can be:

- A permanent, formal, and internal structure
- An ad hoc team pulled together rapidly when an incident occurs
- An external or contracted third-party service organization
- Vendors may have an internal CSIRT that handles mitigation and remediation of vulnerabilities within their own products

The types of CSIRTs that exist are:³

- International coordination centers
- National teams
- Network service provider teams
- IT vendors
- Corporate teams

For the purposes of this book, the focus is on the development of a corporate team. Keep in mind, however, that it is likely that the corporate team may be required to coordinate for support from the first four types of CSIRTs listed above.

The responsibilities of the CSIRT, as defined in the *List of CSIRT Services*⁴ on the CERT® Web site, groups CSIRT services into three categories: (1) reactive services, (2) proactive services, and (3) security quality management services.

Reactive services are initiated when there is an indication that an event is occurring. This may be a report of a virus, malicious code, compromised host, or intrusion that is or has taken place. The core component of CSIRTs are reactive services. The CERT® began as a reactive group. It has since developed into an organization with proactive, reactive, and security quality management services. Most organizational CSIRTs begin with reactive objectives in mind and can or may develop into a permanent structure offering all three services and responsibilities. Reactive services include alerts and warnings, incident handling, vulnerability handling, and artifact handling. For the purposes of this chapter, the focus is on the reactive functions of the CSIRT.

Proactive services are assistance provided in anticipation of an event, attack, or compromise. They are services offered before an event has occurred. Proactive security services were discussed in previous chapters. The proactive services of CSIRTs primarily include monitoring and

detection, as discussed in Chapter 7. Other proactive services might include security program development, penetration testing, security configuration management, research, documentation, and security information dissemination, all topics of other chapters.

Security quality management services are defined by the CERT®/CC as augmentation services that are typically handled by other areas of the organization such as audit, IT, telecommunications, business continuity/disaster recovery, or training departments. Security management services that augment the CSIRT include risk analysis, business continuity and disaster recovery planning, security consulting, awareness building, security training, and security product evaluation, certification, and testing.

The specific responsibilities of CSIRTs may include the following:⁵

- Receive incident data.
- Publish advisories or alerts.
- Perform security policy development.
- Track and trace intruders.
- Perform artifact handling.
- Perform virus handling.
- Filtering network traffic.
- Provide and answer a hotline.
- Patching and repairing systems.
- Rebuild systems.
- Monitor intrusion detection systems (IDSs).
- Produce technical documents.
- Perform training and security awareness.
- Perform research on security vulnerabilities.
- Perform forensic evidence collection and analysis.
- Pursue legal investigations.

Reactive Services

The CERT/CC lists the specific reactive services as follows:

- Alerts and warnings
- Incident handling
- Vulnerability handling
- Artifact handling

Alerts and Warnings

Alerts, warnings, and advisories provide users with descriptive information on an attack, vulnerability, intrusion alert, computer virus, malicious code, or hoax and provide recommendations and guidance for protecting systems as well as recovering from a successful attack or event. These alerts, warnings, and advisories may originate from the internal CSIRT or

be passed from other CSIRTs, security organizations, or vendors. It is important to check the origin and validity of alerts and warnings and ensure that the information is not a hoax.

Incident Handling

The SANS definition of an “incident” refers to an adverse event in an information system or network, or the threat of an occurrence of such an event. The Army Computer Emergency Response Team (ACERT) defines an incident in more detail:

“...an assessed event of attempted entry, unauthorized entry, or information attack on an automated information system (AIS). It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users’ knowledge, instruction, or intent.”

Two key terms related to an incident are: (1) intrusion and (2) event. An intrusion is a subset of an incident where the intruder has successfully gained unauthorized entry into an AIS, or has successfully exceeded access on an AIS. An event is a subset of an incident that contains the specific connection details of the incident, such as times, services, ports, and protocol information. An incident can contain many events.

The term “incident response handling” relates to three functions:

1. Incident reporting
2. Incident analysis
3. Incident response

Incident reporting includes receiving reports or indications that an event is occurring or has occurred. Reporting typically occurs when an anomaly is present in a system or network. Reports can be received via e-mail from a user, as a problem call to a call center or help desk, discovery during routine IT department or network operations, or as a report from an intrusion detection system (IDS).

Incident analysis is the examination of available information, evidence, or artifacts related to an event. This analysis includes identifying the range of the incident and the extent of damage caused to a host, system, or systems, its origination, and potential solutions or fixes. Analysis continues with the correlation of events, and a comparison of similar incidences, patterns, trends, or intruder signatures. The CERT/CC lists two services under incident analysis: (1) forensic evidence collection and (2) tracking and tracing. They are discussed in greater detail later in this chapter.

Incident response begins once information is known about the events of the incident. It is necessary to take and use that information to quickly

react or “respond” to contain or minimize the damage or loss. Incident response may include direct on-site assistance to repair and recover affected systems. It may also be indirect off-site assistance conducted by telephone, e-mail, or fax. Off-site support can include the interpretation of data collected and identifying and relaying recovery strategies to the on-site team. It also includes coordination between the users affected by the incident, other sites involved in the incident or requiring assistance, IT service providers, Internet service providers (ISPs), system and network providers, and other CSIRTs.

Vulnerability Handling

Vulnerability handling includes vulnerability analysis, vulnerability response, and vulnerability response coordination. A vulnerability is any component, software or hardware, that contains a weakness or exposure. Vulnerability handling includes receiving information on hardware and software with configuration weaknesses and exposures, performing technical examination of the characteristics and mechanics of the vulnerability, and developing a plan to fix or reduce the risk of the vulnerability through mitigation techniques. Vulnerability analysis includes reviewing source code, using debugging tools, and reproducing vulnerabilities on test environments. Patches, fixes, or workarounds are then developed. In the case where a vulnerability is not new, it should be researched and appropriate patches applied. The discovery of new vulnerabilities should be reported and coordinated through other CSIRTs and vendors. Patches and fixes, when developed, must then be sent out to the user community so that they can be appropriately applied.

Artifact Handling

An artifact is a file or object on a system that is being used to exploit that system. It may be a valid piece of code that contains an exploitable characteristic, or it may be a file or object that is suspected of being placed on the host during unauthorized activities. Examples of suspect files include Trojan horse programs, toolkits, worms, exploitable scripts, or other malicious code.

Artifact handling includes artifact analysis, artifact response, and artifact response coordination. A vulnerability differs from an artifact in that a vulnerability is valid code with a weakness. An artifact can also be valid code but it has been exploited in an attack or incident and is now part of an investigation or inquiry. It is likely that what was once valid code is now corrupt and will need to be removed from the system, cleaned, or restored. Analysis includes a technical examination of the artifact for file type and structure, comparing valid code to the corrupted code or disassembling the code to understand its function. Once analysis has taken place, a strategy for

INFORMATION SECURITY ARCHITECTURE

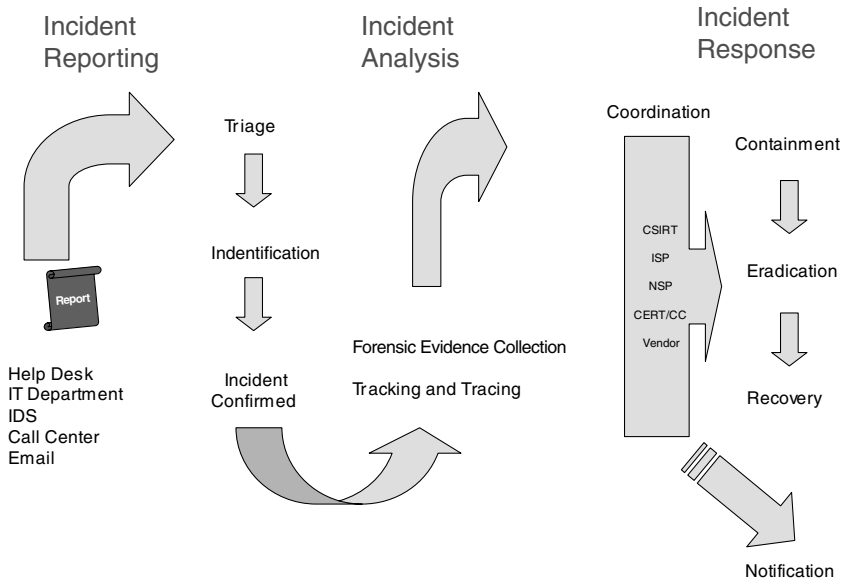


Exhibit 8-1. Incident Response Handling Methodology

removing the artifact from the system and preventing continued or future exploitation must be developed. This is part of artifact response. As in vulnerability response coordination, artifact response coordination is the process of sharing with other CSIRTs, vendors, and the user community, an effective process for cleaning, removal, and protection.

Incident Response Handling Methodology

It was already mentioned that the core component of a CSIRT is reactive services. The core component of the Corporate Team CSIRT is the incident response handling service. The next section focuses on this service.

There is not a standard methodology for incident response handling. The CERT®/CC, FIRST, and other national, international, and governmental CSIRTs are making efforts to establish standards. Exhibit 8-1 above is an attempt to simplify the incident response handling service and its functions through graphical representation. This representation combines some of the ideas of the CERT®/CC methodology with that used by the Army CERT (ACERT) and other Department of Defense CSIRT organizations.

Exhibit 8-1 shows the functions of incident response handling as incident reporting, incident analysis, and incident response. These three functions are listed in bold at the top of the exhibit. If one follows the process, one will find the following sub-functions under each of the three functions listed above:

- Reporting
- Triage
- Identification
- Forensic evidence collection
- Tracking and tracing
- Coordination/external support request
- Containment
- Eradication
- Recovery
- Notification

This chapter section is designed to take the reader through each sub-function in greater depth. Under incident reporting, the diagram shows an anomaly or problem reported through several possible channels. If a formal help desk or call center is not operational, it is likely that the IT department will receive the problem call.

Reporting

The precursor for implementation of a CSIRT is well-defined procedures and processes established to handle trouble tickets or problems. This is usually the defined mission of the help desk. For the purposes of this chapter, we assume that a formalized process is in place to deal with software- and hardware-related problems. Typical day-to-day problems that are called in or e-mailed to the help desk include:

- Requests for assistance with applications
- The inability to log on to a system
- Forgotten passwords
- Change password requests
- Application and network access
- Unavailability of system resources
- Lost data
- Frozen hard drives
- System crashes
- Virus notifications

This is not an all-inclusive list. Many of these requests, with the exception of virus notification, will be accidental or unintentional human error or system failure. On the other hand, all of them except application assistance could be an indication of an incident.

The main purpose of a help desk is to provide centralized assistance with day-to-day operational and technical problems and requests. The services that a help desk provides are defined in its mission statement, as discussed in Chapter 7. As with the CSIRT, the services provided should be defined in the CSIRT's mission statement. It is common, however, to see an

overlap in the reporting and identification functions of the help desk and CSIRT. A typical mission statement for a help desk is to provide end-to-end problem resolution for desktops, servers, networks, and applications. This would imply that the help desk plays a role in problem resolution for incidents and any effect they have on desktops, servers, networks, and applications.

The help desk is most often the first point of acknowledgment for an event related to an incident. For this reason, help desk personnel should have some training and technical experience with incident response so they can appropriately identify suspicious activity, anomalies, and events that are strong indicators of an incident. In many cases, help desks will perform some CSIRT functions in the absence of a formal CSIRT structure. Logically, the help desk would provide membership on the ad hoc Corporate CSIRT. This is discussed later in the chapter.

The help desk typically has its own problem tracking software to document, track, and close requests for assistance. When a serious incident or event is suspected, information or reports from the help desk problem tracking software should be forwarded to the CSIRT, along with the following information in an incident report. The incident reporting form in Exhibit 8-2 has been patterned after the Department of Defense (DoD) CERT Incident Reporting Form.⁶

When additional information about events or the incident becomes known, subsequent follow-up reports should be submitted. Exhibit 8-3⁷ provides an example of a follow-up report. This form is very similar to the initial incident reporting form but is intended to document and report the technical details that have become known during the course of the incident or analysis process.

Information that should be included when reporting an incident are:⁸

- Tracking numbers (Internal to the organization)
- Tracking numbers (of other CSIRTs)
- Keywords or categorizations
- Contact information
- Policies
- Priority
- Other materials (associated with the incident)
- Incident history
- Status
- Actions
- Incident coordinator
- Quality assurance parameters
- Textual descriptions

Exhibit 8-2. Incident Reporting Form

**Starcross CSIRT
Incident Reporting Form**

This form meets the initial reporting requirements outlined in Starcross Security Policy 5.3 to report computer or network events. E-mail this form to starcross@starcross.net. If you are unable to e-mail this form, you may send it by fax to (412)555-5567. For virus reporting, please use the virus reporting form on the Starcross home page to submit detailed virus reports.

Report Classification: For Official Use Only (FOUO)

From: CSIRT Tracking #:
To: Starcross CSIRT (Assigned by CSIRT)
Date/Time of Incident:
Type of Incident:
 Probe User Level Access
 Scan Root Level Access
 DNS Malicious Logic
 Denial of Service

Name of Asset:
(Machine Name)

Mission Impact:

Details of Incident: (See Reporting Guidelines for more detail information.)

IP Address of Source (i.e., xxx.xxx.xxx.xxx):
Machine Function:

- | | |
|--------------------------------------|--|
| <input type="checkbox"/> Web Server | <input type="checkbox"/> Multi-function Server |
| <input type="checkbox"/> DNS Server | <input type="checkbox"/> Router |
| <input type="checkbox"/> File Server | <input type="checkbox"/> Firewall |
| <input type="checkbox"/> Mail Server | <input type="checkbox"/> Workstation |

Date and Time of Incident:
IP Address of Destination (i.e., xxx.xxx.xxx.xxx):
Where:

Why:

Action Taken:

Contact Information:

Coordination:

Exhibit 8-3. Follow-Up Incident Reporting Form

**Starcross CSIRT
Follow-on Incident Reporting Form**

1. The Follow-on Incident Report Format will be used for all subsequent reports. This format includes the raw details needed for regional teams to understand the technical nature of the problem and will be merged with information obtained from other reports to highlight regional trends. Normally, this form will be forwarded by secure e-mail or any of the approved reporting methods. The form is available at <http://www.starcross.net>.
2. Starcross CSIRT will provide feedback to reporting organization as more information becomes known. Feedback will flow back through the incident reporting structure. Subordinate layers in the reporting channels are responsible for relaying this information to the originating point, and for developing procedures to disseminate the information as appropriate within their constituent communities. This format is also used by CSIRT organizations to report information developed through observation, correlation, analysis, or other means. Please feel free to duplicate any section as required. Please return this form to starcsirt@starcross.net. If you are unable to e-mail this form, please send it by FAX to (412)555.5567.

Report Classification: For Official Use Only (FOUO)

From: CSIRT Tracking #:
To: Starcross CSIRT (Assigned by CSIRT)
Date/Time of Incident:
Type of Incident:
 Probe User Level Access
 Scan Root Level Access
 DNS Malicious Logic
 Denial of Service

Name of Asset:
(Machine Name)

Mission Impact:

Technical Details of Incident:

Action Taken:

Contact Information:

Coordination:

It is important that CSIRT members understand that a new report does not necessarily indicate a new incident. A review of both open and closed reports increases awareness of leading factors that establish patterns.

Incident Classification

The information gathered from a report will assist in properly classifying an incident. Classifications enable the exchange and comparison of computer security incident information. Incidences can be broadly categorized as intrusions, denial-of-service attacks, malicious logic, or probes. These have been defined previously throughout this book. Below are brief definitions that will help the reader compare and understand the differences when categorizing an incident.

1. *Intrusion*: unauthorized access to an information system.
2. *Denial-of-service (DoS) attack*: actions that prevent a system from functioning in accordance with its intended purpose and that can cause destruction, modification, or delay of service.
3. *Malicious logic*: hardware, software, or firmware placed in an information system for unauthorized purposes such as damage, destruction, or unauthorized access. This includes malicious code, viruses, Trojan horses, and worms.
4. *Probe*: any attempt to gain information about an information system or its users online. The types of probes are war dialing, sniffing, and footprinting.

These four categorizations can be subcategorized into serious, significant, or simple. Subcategorizing depends on the sensitivity of the information or system accessed, the number of attempts on the system, and the extent of damage. There are two other categorizations in use:

1. *Unknown*: category for an incident that is of an undetermined source or characteristics.
2. *Hoax*: invalid or false warning regarding potential incidences.

While hoaxes are seemingly harmless, they expend considerable employee productivity when administrators concentrate their efforts on analyzing false problems. They have also caused users and administrators to delete files and reload operating systems and applications.

Classifications assist in the comprehensive and systematic incident analysis process. Standardized, refined, and accurately catalogued information enhances the database capabilities of CSIRT entities, both governmental and nongovernmental.

Triage

The CERT®/CC defines triage as a function of incident reporting. Triage is the central collection point for all information received on an incident. Triage

provides for a single entity to accept, collect, sort, order, and pass all incoming information. Triage in medical terms allows the assessment of severity of an injury so that the most critical lifesaving methods can be administered. For example, if an individual is brought into the emergency room with a broken leg, a gun shot wound to the chest, and a crushed arm, triage is the assessment of the three wounds and the determination that the one that is going to be a showstopper is the chest wound. It would be ridiculous to start setting the broken leg when it is obvious that ignoring the gunshot wound to the chest will result in death. The injuries are prioritized so that the response to the injuries will be appropriate. The same function exists for the CSIRT. The information must be collected and quickly assessed, sorted, and prioritized so that the most critical events can be addressed to minimize loss and damage.

CSIRTs must advertise a single point of contact. In the example forms above, this is shown as `starcsirt@starcross.net`. There are no individuals listed, simply a single entity. This ensures that all pertinent information is being received quickly through a single channel or point of contact. Additionally, forms must be easy to use and understand to make the collection and reporting of all relevant information effective. Forms should include:⁹

- A clearly defined point of contact
- Specific details on the availability of the defined point of contact
- Simple but defined procedures to follow
- Clear guidelines on the kind of events to report
- Supporting documentation (e.g., reporting forms and references to other available documentation) for reporter's use

When incident reports and information are received, an acknowledgment of receipt should be sent. The information will then be sorted, ordered, and sent to the appropriate individuals performing analysis. Information must be compared to previous reports for correlation of events. If events are related, they must be tracked as a part of the same event; otherwise, they are assigned as a new event.

A tracking number is the tool used to identify a particular incident. Standard tracking numbers with prefixes can identify the type of "event," such as an incident, vulnerability, or information. The CERT[®]/CC uses the prefixes "CERT#" to identify an incident, "VU#" to identify a vulnerability, and "INFO#" to identify information or announcements. Part of the tracking number can be used to identify the CSIRT team handling the incident. Another prefix can be used to identify a particular incident, while a third part of the number can be used to identify the event related to that incident. An example is:

CERT#-001-0025-0003

This example indicates that the information is classified as an incident given to Team 1 and is the third piece of information related to incident number 25. This example is used only to illustrate the use of prefixes and identifiers. It is not a standard. Tracking numbers should be unique. Ranges of numbers to identify CSIRT services and functions are also used to eliminate confusion. For more information on the use of tracking numbers, refer to *the Handbook for Computer Security Incident Response Teams (CSIRTs)*.¹⁰ Another reference that is an attempt to standardize how incident information is reported, tracked, and archived between CSIRTs is “TERENA’s Incident Object Description and Exchange Format Requirements” (RFC 3067).

Identification

Although similar to the CERT®/CC, the Army CERT (ACERT) describes incident response handling functions as:

1. Identification
2. Containment
3. Eradication
4. Recovery

In the incident response handling flow diagram in Exhibit 8-1, identification falls under the function “incident reporting.” The next three functions — containment, eradication, and recovery — fall under “incident response.”

Identification is the determination of whether or not an actual incident has occurred. It is not uncommon for a user to think he has been subjected to a virus, attack, or unauthorized access to their account, only to find that the incident is not a hostile act but simply a user error, outdated code, configuration error, hardware failure, or miscommunication. Identification includes the steps taken to narrow and eliminate the possibilities. Identification begins when an anomaly in the system is recognized. The central point of control of the event and analysis is designated as the triage function. As Exhibit 8-1 shows, this may begin with the help desk or call center if one exists. An individual or individuals with expertise in incident response handling can usually eliminate the benign issues listed above rather quickly and make the determination that an actual incident is in progress.

The identification process begins after triage, when information and reports are received and there is an indication that an event is more than just a daily operational problem or error. At this point in the flow diagram, some potential incidences will turn out not to be incidences and others will. Once enough information is received to confirm a potential incident, the “incident analysis” function begins, as shown in the middle of Exhibit 8-1.

Note that there is a gray line between incident reporting, incident analysis, and incident response. The help desk performs some high-level analysis to determine if a problem is an incident and should be reported. Also, all three functions should happen quickly and therefore may occur concurrently. Reporting does not end so that analysis can begin. Analysis does not end so that response can begin. They can continue simultaneously. Triage, identification, and incident confirmation are shown in Exhibit 8-1 between reporting and analysis because of the concurrency of the functions.

Incident Analysis

In-depth incident analysis focuses on the technical analysis of log files, malicious code, and techniques used in the incident. Functions of incident analysis include:

- Examining log files
- Analyzing software on affected components
- Identifying affected sites
- Researching technical documents and advisories
- Providing technical support throughout the analysis process
- Providing advice and assistance on workarounds until the incident is understood
- Providing on-site assistance

The CERT/CC categorizes incident analysis as forensic evidence collection and tracking and tracing. Forensic evidence collection is “the collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise.”¹¹ In so doing, a provable chain of custody must be maintained for any evidence collected.

A provable chain of custody is the documentation necessary in a court room that substantiates the evidence through a known series of events that are documented and time/date stamped with proof that the evidence was not tampered with or out of the control of the individuals with authority to perform incident response handling. At the point where a chain of custody is necessary, it is wise to get legal counsel involved for advice and guidance. Videotaping the archival process of evidence is wise. Archiving includes numbering, dating, and signing every piece of information, including log files from computers, IRH notes, configuration printouts, screen prints, and connection logs. The originals of all information should be sealed in envelopes or containers that are numbered, dated, and signed. As this evidence is turned over to differing individuals of authority, it should be signed for and logged. Access to secure containers holding evidence should be limited to a small group of individuals who understand, through policy, the necessity to control access. Proof of access and key control is

necessary. Team members who discover, analyze, or hold evidence of an incident may be called into court as expert witnesses.

Forensic evidence collection includes performing the following tasks:

- Making bit-image copies of affected hard drives
- Checking for changes to the system
- Identifying the addition of new programs, files, or users to the system, including Trojan horses and toolkits
- Reviewing running processes and open ports

Tracking and tracing is the analysis made to determine the origin of an attack. This includes identifying all systems affected or used to gain access, the points of entry into an internal network, external networks, and Internet service providers (ISPs) also used in the attack. Tracking and tracing is working logically backward to the starting point or origination of the attack and potentially learning the identity of the intruder. In many cases, the origin of the intrusion will lead to other networks and systems outside the components owned by the organization. Tracking and tracing may then become a coordinated effort between other CSIRTs, ISPs, network providers, and vendors.

Most hardware, applications, and operating systems contain log files. Log files are designed to provide a history of the processes that take place during operation and are used to analyze errors, test code, improve configurations, and trace intrusions. Log files are often used in conjunction with alerts and alarms designed to notify the system administrator of a problem within the system. Alarms occur when predefined criteria are compared to and match an event in the log file.

Log files provide such information as:

- Destination and time of user login
- Type of login (SSH, telnet, rlogin, etc.)
- Destination of e-mails
- Errors
- Unauthorized access attempts
- Changes to configuration

To be useful and valid in incident analysis, log files should contain the following:

- Time stamps for each event
- Internet name
- Network address
- Machine type
- Software and version number
- Configuration files used to generate the logs
- Method of authenticating the validity of the log

Log files will often contain sensitive information such as user ID and password combinations, e-mails and their attachments, employee names, machine names, and network addresses. Log files should be categorized based upon the sensitivity of information they contain. Secure transmission of the log files should correspond to the sensitivity categorization. For example, the information just listed should be transmitted over encrypted links. Access to files that are part of evidence should be protected and controlled for use during litigation as described above under chain of custody. Irrelevant information and log files should be properly disposed of because the information contained within them provides insight into the systems.

According to the CERT/CC, analysis is categorized into two sub-functions: (1) intra-incident analysis and (2) inter-incident analysis. Intra-incident analysis is the examination of artifacts, software, and the web-of-trust related to a specific incident. Inter-incident analysis is the correlation of separate incidences, determining similarities and potentially the same source or related sources of intrusion activity. This type of analysis provides a broader picture and includes the examination of trends, statistics, and case studies. It also enables the development of a knowledge base that can be used to predict and thwart future similar events through refined and improved response procedures and lessons learned. The depth of analysis is important to consider.

Incident Response

Once information is known about the events of the incident, it is necessary to take and use that information to quickly react or “respond” to “contain” or minimize the damage or loss. Exhibit 8-1 lists the functions under incident response as coordination, containment, eradication, recovery, and notification. These will be covered in the following paragraphs. The CERT/CC translates incident response functions into three basic services:

1. Incident response on-site
2. Incident response support
3. Incident response coordination

Incident response on-site is defined as the activities of the team members to physically remove artifacts from desktops, servers, and any components involved in the incident and to restore operational capabilities of those components to their original state.

Incident response support is off-site assistance provided through telephone, fax, or e-mail to provide guidance and assistance in report or data analysis and the recovery methodologies. An example of off-site support would be if a corporate CSIRT contacts the CERT/CC regarding a specific incident requesting assistance. The CERT/CC may ask that incident reports

be e-mailed along with component logs. The CERT/CC may then classify a particular incident according to similarities of other incidents reported nationally or internationally. The CERT/CC may determine that the incident reported has identical characteristics to a new malicious code, for example, the W32/Blaster Worm. On August 11, 2003, the CERT/CC issued advisory CA-2003-20 related to the W3/Blaster Worm. This advisory describes the characteristics of this malicious code and its known exploit capabilities of a vulnerability in Microsoft Remote Procedure Call (RPC) Interface. The corporate CSIRT can use the recovery strategy described in the CERT® Advisory to begin its recovery on the components affected. The on-site team need not develop its own strategy but can rely on the research efforts of the CERT/CC and other national or international CSIRTs and their experience with this particular incident.

It is important to note that the example above is a simplistic view of off-site support. The CERT/CC is not designed as a support mechanism to any corporate CSIRT. It has a charter that defines its responsibility to the Department of Defense (DoD). Organizations can solicit CERT/CC support; however, the CERT/CC's priority will be to respond to DoD, governmental organizations, and other institutions supporting the national infrastructure.

Incident Response Coordination

It is important to document and understand all of the related organizations that will be a part of the CSIRT coordination and notification. This includes victims of the attack, other sites that may have been used in the attack but not necessarily damaged by the attack, and any site requiring assistance. It also may include information exchange, analysis, and collaboration with IT service providers, vendors, network and system administrators, ISPs, legal counsel, human resources departments, public affairs departments, law enforcement, and other CSIRTs requiring involvement. If your organization provides electricity to the Eastern seaboard, it is more than likely that you will be dealing with the Computer Incident Advisory Center (CIAC), the Department of Energy's CSIRT.

Coordination is the first step in the incident response function. As one can see from Exhibit 8-1, coordination occurs at the beginning of incident response; during all other functions of incident response such as containment, eradication, and recovery; and in conjunction with notification. Coordination involves gathering contact information, notifying potential sites of their involvement in the incident, collecting statistics, and facilitating information exchange and analysis. Information coordinated will also include fix and mitigation strategies. Below is a list of key organizations that may become part of your organization's coordination and notification function.

Key Organizations

It is necessary to emphasize that the first CSIRTs were developed in the effort of cooperation and coordination to share response strategies and early alert capabilities to potential problems. The following organizations are willing to share their research, knowledge bases, best practices, and lessons learned in an effort to provide effective and secure networks and computer systems for the betterment of business and the community. Those organizations include:

- *CERT® Coordination Center (CERT®/CC)*. Located in Pittsburgh, Pennsylvania, at the Carnegie Mellon University Software Engineering Institute (CMU/SEI), the CERT/CC studies Internet security vulnerabilities, provides incident response services to sites that have been the victims of attack, publishes a variety of security alerts, researches security and survivability in wide-area networked computing, and develops information to help improve site security. The CERT advisories, bulletins, summaries, and frequently asked questions (FAQs) can be found at the CERT Index at: <http://www.cert.org/contents/contents.html>.
- *Computer Incident Advisory Center (CIAC)*. The CIAC serves the Department of Energy (DOE) and is one of the two oldest response teams, established in 1989. It is nationally and internationally recognized for its contributions to the Internet community. The CIAC's mission is to apply cyber-security expertise to prevent, detect, react, and recover from cyber incidences for the United States. It is a founding member of FIRST. The Web site can be found at: <http://www.ciac.org/ciac/>.
- *Federal Computer Incident Response Center (FedCIRC)*. The FedCIRC is the federal civilian government's organization that provides computer security incident reporting, and assistance with incident prevention and response. As of March 1, 2003, the FedCIRC became part of the Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) Directorate. This Web site originally established at: <http://www.fedcirc.gov/> has since migrated to the Department of Homeland Security Web site at: <http://www.dhs.gov>.
- *Forum of Incident Response and Recovery Teams (FIRST)*. FIRST is a coalition of government, commercial, and academic organizations specifically developed for the cooperation and coordination of incident response and security teams. It began in August 1989 as an invitational workshop organized by the CERT®/CC to coordinate relationships between other CSIRTs and discuss best practices, and was formalized in November 1990. Members work voluntarily, continue to improve the existing coordination network, and concentrate on prevention of incidents, sharing information, sharing vulnerability and forensic analyses, and coordinating response activities when

incidences occur. The original 11 founding members of FIRST have now grown into 151 members as of September 2003. The FIRST Web site is at: <http://www.first.org>.

- *National Infrastructure Protection Center (NIPC)*. Created on February 26, 1998, from recommendations of the President's Commission on Critical Infrastructure Protection, the NIPC is a product of the Department of Justice and the Federal Bureau of Investigation (FBI) and is located at FBI Headquarters. It is a joint endeavor between both government and private sectors and includes representation from federal, state, and local governments. It is the national focal point for threat assessment, warning, investigation, and response to attacks on critical infrastructures. The NIPC Web site can be found at: <http://www.nipc.gov>.
- *US Computer Emergency Response Team (US-CERT)*. The US-CERT was created on September 15, 2003, by the Department of Homeland Security and in conjunction with the CERT[®]/CC and works with the National Cyber Security Division (NCSA). The US-CERT is designed to utilize the CERT/CC's capabilities to accelerate the nation's response to cyber-attacks and vulnerabilities. The US-CERT Web site can be found at: <http://www.us-cert.gov/>.

There are many Department of Defense organizations and programs whose Web sites may or may not be readily available via the Internet. A majority of these sites can only be accessed through valid government TCP/IP addresses. Nonetheless, they are excellent sources of tools, research, whitepapers, secure configuration guidance, and lessons learned. These organizations include:

- The National Security Agency/Central Security Service (NSA / CSS)
- Information Assurance Centers of Academic Excellence
- The Defense Information Systems Agency (DISA)
- Department of Defense Computer Emergency Response Team (DoD-CERT)
- The Defensewide Information Assurance Program (DIAP)
- The DoD Information Assurance Program
- Naval Computer Incident Response Team (NAVCIRT)
- Air Force Computer Emergency Response Team (AFCERT)
- Army Computer Emergency Responses Team (ACERT)
- The Land Information Warfare Activity (LIWA)
- The National Guard Bureau CERT Coordination Center (NGB-CERT/CC)

Containment

As stated previously, containment is part of the incident response function. The objective of containment is to keep the situation created by the incident from getting worse by limiting its scope and magnitude. Teams deployed for on-site assistance should take care to not increase damage by

INFORMATION SECURITY ARCHITECTURE

acting too quickly before analyzing pertinent information. Care should also be taken not to damage evidence. Steps in eradication include:

- Secure the area.
- Collect information using predefined survey forms.
- Review and analyze information collected in the identification phase.
- Do not alter systems until a backup is performed.
- Perform backups immediately using new media.
- Collect and analyze log files.
- Check all and any conclusions reached by others.
- Maintain a low profile so as not to alert the attacker.
- Maintain standard operating procedures.
- Make the determination if systems should be shut down, disconnected from the network, or operate as normal.
- Recommend system password changes.

Appendix D contains an example of an intrusion checklist that can be used in the containment phase. Rookie CSIRT team members often make the mistake of using common techniques to identify the attacker, thereby alerting him that he has been discovered. These common techniques include ping, nslookup, finger, and telnet. Today's attackers are more savvy and educated and will delete file systems and break off contact to cover their tracks. A full backup should be made as soon as there is any indication that an incident has occurred or is occurring. New media should be used to eliminate writing over old data. A backup initiated immediately can be compared to later backups to determine if any additional unauthorized activity has occurred.

Acquire network and computer logs immediately. Many log files turn over quickly and critical evidence or clues can be lost. Logs will indicate whether the attack is internal or external. The most difficult decision will be deciding whether to turn off the system completely, disconnect it from the network, or continue to operate normally to monitor system status. This decision receives extreme pressure by end users and senior management. If it can be determined from the files that the attack is external, a strong consideration should be made to isolate the organization's network from the Internet at the firewall. For internal attacks, subnets can be isolated at the router. Logs and file signature databases from other systems on the same subnet should be reviewed. Other systems that have an established trust relationship with the affected system(s) or routinely connect to the affected system(s) should also be reviewed.

Continue to follow standard operating procedures. This may include the use of intrusion detection systems. These systems are designed to break connections and block attacking IP addresses. During containment, it is tempting to disable such systems to provide a better trace of the intruder.

It is wise to keep such systems enabled and monitored. Disabling such systems can alert intruders that they have been discovered.

System owners should be extremely sensitive during this process for several reasons: (1) business may stop and large amounts of time and money can be lost; (2) end users will need the system for important projects and business; and (3) system owners will feel a sense of responsibility, fault, or blame for the incident. For these reasons it is important to keep the system owner informed of the status of the investigation. It is also important to not place blame or fault during the investigation, as system owners tend to become defensive. It is also necessary to mention to system owners the things that have been done right.

Eradication

The objective of the eradication phase is to eliminate the problem and close the point of entry of the attack. The only way to eliminate a problem is to understand how it occurred in the first place. The information collected in earlier phases of incident response handling will be used, as well as other information gathered during eradication. An attack should be isolated to determine how it has occurred. Sometimes, the exact mechanism used in the attack cannot be determined. In this case, a list of possibilities should be documented.

Once the cause of the incident has been determined, steps are taken to remove it. This poses a challenge to the organization. The solution to viruses is simply to remove them from all media using commercial software. Companies that produce virus eradication software have a very quick turnaround time for new viruses and publish signature files and fixes within a matter of days after discovery.

Network intrusions are not so simply repaired. Backdoor software or tools such as sniffers are often installed by intruders so that they can continue to access the network and systems. It is the responsibility of the CSIRT to search for all such programs and remove them. Where there is evidence of a root-kit attack, it is often necessary to reformat drives, rebuild operating systems, and reinstall all applications from their original source.

Some attackers, once they know they have been detected, will continue to attempt to maintain control of the systems despite eradication efforts. In such cases, law enforcement officials should be notified. The CSIRT team must trace the attack, contact administrators of other networks being used in the attack, and attempt to gain their system, network, and phone logs.

Password files and system identity are often publicized after an attack. This increases the likelihood that the system will be subject to follow-on attacks for weeks. Firewalls and router configurations should be analyzed

and modified. Systems can be moved to a different address space or the machines can be ported to a more secure operating system.

A network and system security assessment and vulnerability analysis should be performed to identify additional vulnerabilities. Vulnerabilities that have been exploited or identified on the system should be checked on other systems throughout the organization.

Recovery

The objective of the recovery phase is to restore the system to full operational status. In some instances, a full restoration of a backup is required. It is necessary to ensure that the backup itself does not have any integrity issues. Often, backups contain remnants from the intrusion. It will be necessary to determine the last backup prior to the initiation of the attack or compromise. This is also an optimal time to apply system patches.

The CSIRT along with system owners and administrators must verify that the restoration was successful and that the system has been restored to normal operation. Organizations should already have system test plans in place to evaluate the system. If there is no test plan, then one should be developed at this time. Test plans include closely monitoring network and system logs while the system runs through its normal operational tasks. If additional system patches or upgrades have been installed, it is likely that the system will function differently than before the intrusion. Once a system is back online, the system should be monitored for back doors, tool-kits, or malicious code that has escaped detection.

Follow-up is a function of the recovery phase. Follow-up identifies lessons learned that can be used to improve the CSIRT's incident handling capability. It also is the function that provides support to the litigation process against attackers. A follow-up report should be initiated with input from all parties participating in and affected by the incident. The report should be reviewed by affected parties. Afterward, a meeting should be conducted to provide education, training, and improvement to the CSIRT process.

The incident should be summarized in an executive summary for management that includes the costs of time and money spent dealing with the incident as well as its impact. The executive summary should include recommended changes derived from the lessons learned process. These recommendations should include related costs of their implementation, an implementation schedule, and the risks and impact of not following the recommendations.

Notification

Notification is the process of passing appropriate response and recovery information to constituents, other affected sites, and CSIRTs. In the general

sense, notification is the process of keeping those potentially affected by an event or incident informed. The CSIRT/CC lists this as the announcement function. Compared with the coordination function previously discussed, notification occurs when there is enough information and validation about events and incidences to make recommendations to others affected or potentially affected by those events and incidences. The main objectives for notification and announcements are to disclose information to those affected, to assist them in protecting their systems, or to provide warning of a potential attack by identifying past, current, or present threats.

CSIRT/CC lists the types of announcements as:

- Heads-up
- Alert
- Advisory
- For Your Information
- Guideline
- Technical procedure

The categorizations listed above are slightly different in the amount, type, and status of information provided. A heads-up announcement is a short message issued when detailed information is unavailable.¹² It provides a warning of an event that may occur in the near future. The benefits of a heads-up message are threefold: (1) it provides awareness of a potential threat to users, (2) it gives users the opportunity to respond with additional information that the CSIRT may not know or currently have, and (3) it puts the user in a better position to recognize information of potential importance. A characteristic of heads-up notices is that information contained in the notice will inevitably change.

The next type of announcement is an alert. “Alerts are short-term notices about critical developments containing time-sensitive information about recent attacks, successful break-ins, or new vulnerabilities.”¹³ Alerts are typically initiated when new information has been received and needs dissemination. Many anti-virus software companies will send alerts to their clients when a new virus has been reported. These alerts often prompt the user to “download virus updates now.”

Advisories are well-researched notifications that provide mid- and long-term information regarding problems and solutions. They are designed to provide awareness and help to avoid incidences. Advisories contain more technical detail about fixes, patches, and work-arounds, and are aimed at system and network administrators. They are published most often regarding new vulnerabilities but can also provide information about recent intruder activity.

For your information notifications contain mid- and long-term information targeted at a less technical audience. The CSIRT/CC provides this type

INFORMATION SECURITY ARCHITECTURE

of information in “Bulletins.” This information can be documented as well in newsletters and is of a more tutorial or instructive nature.

Guidelines are step-by-step procedures designed for an individual whose responsibility it is to implement a specific day-to-day practice (i.e., system and network security). Guidelines are designed to expand the implementer’s knowledge of that topic and can be lengthy in nature. Many guidelines can be found at www.cert.org, and include guidelines on reporting incidences, Windows NT configuration, UNIX configuration, managing the threat of denial-of-service attacks, implementing site security policies, and developing a risk evaluation methodology.

Technical procedures are lengthy documents aimed at persons considered experts in their field. They contain technical detail usually related to a specific problem or domain. Technical procedures often come from software and hardware vendors and describe step-by-step details regarding modifications to configurations.

A new CSIRT will not typically have the resources to create all of these types of announcements and notifications. Many of these announcements, such as advisories, bulletins, and technical notes, are available on the CERT/CC Web site and through hardware and software vendors. Announcements such as a heads-up, alert, or “for your information” can be created less formally for a local set of users. As your corporate CSIRT develops and matures, the notification and announcement function will become a more advanced, formalized, and well-defined process.

Development of the CSIRT

The CSIRT will vary from organization to organization; however, the structure should include a definition of:

- Mission, goals, and objectives
- Constituency
- Services
- Definitions and terminology

The mission documents what the CSIRT is designed to do and what it is trying to achieve. This mission statement should be defined, documented, and disseminated among the individuals supported by the CSIRT so that expectations of the mission, goals, and objectives are clear to those supported, and the CSIRT can maintain a focus on those goals and objectives. The mission statement defines the CSIRT’s role, purpose, and the framework within which it operates.

The following paragraphs numbered 1 through 3 build an example of a basic CSIRT mission statement. A good beginning for a corporate mission statement might include:

(1) Improve the security of the Starcross information infrastructure and minimize threat of damage resulting from intrusions.¹⁴

This statement can be expanded to define to whom the CSIRT will provide services as shown in paragraph 2 below, and what services will be provided as shown in paragraph 3 below:

(2) The Starcross CSIRT will provide both reactive and proactive services to Starcross end users, subsidiaries, clients, and business partners operating on the Starcross domain.

(3) Reactive services will include alerts and warnings, incident, vulnerability, and artifact handling. Proactive services will include announcements, technology updates, security audits and assessments, intrusion detection services, and security-related information dissemination.

The mission statement should be short, understandable, and provide the scope of responsibilities of the CSIRT. From this mission statement, the CSIRT can begin to derive its services, policies, and procedures. Exhibit 8-4 (CSIRT Mission, Tasks, and Subtasks) is from a Department of Defense (DoD) CSIRT organization training plan. It further defines the tasks and subtasks related to the mission of a CSIRT organization.

The CSIRT also needs to determine the community that it is established to serve. This is known as the constituency. The CERT/CC defines the constituency as “a specific group of people and/or organizations that have access to specific services offered by a CSIRT.”¹⁵ The constituency is typically defined by the funding source for the CSIRT. Other ways to define the constituency are by the organization, suborganization, or by the networks and subnetworks within the scope of a domain or domain names. The scope of the constituency may include geographical, national, international, political, technical, organizational, or contractual boundaries.

In defining the constituency, it is also important to determine the level of authority that the CSIRT has been given to perform its service offerings to the constituency. There are three levels of authority: full, shared, and none. The CERT/CC defines full authority as members of the CSIRT having the authority to undertake any necessary actions or decisions on behalf of their constituency. Shared authority is defined as members of the CSIRT providing direct support to their constituents and sharing in the decision-making process. No authority is defined as members of the CSIRT acting only as advocates or consultants to that constituency without the ability to dictate decisions or actions to its constituents.

The level of authority of the CSIRT team must be understood by the constituency, management, and other technical teams because it will impact the interaction, cooperation, and coordination that is necessary between the CSIRT, other teams, and constituents. If the only individual who can authorize the shutdown of an application is the application owner or department

Exhibit 8-4. CSIRT Mission, Tasks, and Subtasks

Mission

The CSIRT mission is to protect the Starcross IT and automation infrastructure, which includes automated information systems (AIS) and classified and unclassified local area networks (LANs). CSIRT ensures AIS is authorized, protected, and accredited in accordance with DoD 5200.40 Department of Defense Information Certification and Accreditation Program (DITSCAP). CSIRT prepares, distributes, and maintains plans, instructions, guidance, and standard operating procedures (SOP) concerning the security of systems operations, including networks.

Required Tasks and Subtasks

1. Manage compromises:
 - a. Receive trouble tickets from the Regional CSIRT of a verified system compromise (i.e., Nimbda virus, remote anywhere, root compromise, or other severe activity).
 - b. Identify compromised IP space.
 - c. Communicate with POC the details of system compromise to include systems affected, log files, appropriate action, "have fixed" date.
 - d. Communicate compromises to corporate Help Desk, oncoming shift, and CSIRT Security Manager.
 - e. Track status of compromises.
 - f. Receive compromise fix reports from POC on compromised systems.
 - g. Scan compromised IP(s) to validate fix actions.
 - h. Close trouble tickets for compromises. Communicate with POC and appropriate CSIRT, oncoming shift, and CSIRT Security Manager on close status.
 - i. Communicate with the Telecommunications Support Group (TSG) to remove blocks on IP(s) related to fixed compromise.
2. Perform fault isolation during the Identification of System and Network Vulnerabilities.
3. Conduct threat and vulnerability assessments:
 - a. Implement Information Assurance Vulnerability Assessment (IAVA) scans.
 - b. Administrator access required.
 - c. Set up and configure scan software.
 - d. Generate an Internet security scanner (ISS) key.
 - e. Generate assessment reports.
4. Prepare maintain plans, instructions, guidance, and SOPs concerning security of system operations.
5. Password management:
 - a. Generate daily password.
 - b. Set up and implement "Password Creator" software.
 - c. Communicate daily password to appropriate help desk personnel.
 - d. Implement password changes.
6. Implement security management software.
7. Generate and analyze firewall log reports:
 - a. Run firewall logging session.
 - b. Use Excel software to generate spreadsheets.
 - c. Use MS Access to store firewall logs.

Required Training:

Remedy
HP OpenView

Exhibit 8-4. CSIRT Mission, Tasks, and Subtasks (continued)

MS Exchange E-mail
MS Excel
MS Access
Cisco Certified Network Associate (CCNA)
Microsoft Certified Professional (MCP)
Lucent Security Management Software
Internet security scanner
Password generator
Norton Anti-Virus
Real Secure IDS software
STAT Scanner V5.0
Information Assurance Vulnerability Assessment (IAVA) Process
CSIRT Trouble Ticket Process
Network and System Security
Information Operations (IO)
Incident Response Handling (IRH)
Department of Defense Information Certification and Accreditation Program
(DITSCAP)
Department of Defense Information Vulnerability Assessment Program (DITYVAP)

department manager, CSIRT will have to articulate to that application owner the impact of an incident, the impact of continuing to operate the system in light of the incident, and the impact of shutting down the system in light of the incident. That is, the owner will have to articulate to the CSIRT what the business impact will be of shutting down the system. A CSIRT with full authority may decide to shut down a system. Full authority does not preclude the CSIRT from properly coordinating with department managers, system owners, and giving proper notification to the users.

The function of the CSIRT may reside in different parts of the organization. It can be its own organization or the function can reside within the security team, business continuity or disaster recovery, audit, or information technology. The placement will most likely be a function of resources available, the size and complexity of the organization, and the level of risk that exists. Determining where a CSIRT resides is part of the risk management framework. It is necessary to understand the risk management duties and responsibilities of each of the departments responsible for those functions and how those responsibilities interrelate with the CSIRT and each other. Under the risk management framework, it is necessary to consider both technical and business risks. There may be some overlap of responsibilities, especially with the security team. An understanding of the duties and responsibilities of each function will minimize operating in isolation or contradiction to each other.

Issues in Developing a CSIRT

There are several matters to consider when developing a CSIRT. Several of these issues are listed below and will be discussed briefly in this section:

- Funding
- Management buy-in
- Staffing and training
- Policy development
- Legal issues
- Reevaluation of CSIRT operations

Funding

CSIRT implementations will differ greatly, depending on funding, technical expertise, and organizational structure. The major limiting factor related to setting up a CSIRT is funding. Funding will impact the number of staff, physical resources, and training. Maintaining staff with the appropriate technical expertise can be a challenge. Without this expertise, CSIRT staff will have to rely on support services and information generated from other teams. This will degrade the services provided by the corporate team. Funding is typically provided by a parent organization and under the budget of the IT department. Some CSIRTs obtain funding by providing a membership subscription service that charges a fee for its CSIRT services.

The cost of setting up a CSIRT will vary, depending on the size of the organization and the number of services that the CSIRT offers. Because internal organizational CSIRTs are relatively new, few statistics are available to directly answer the question of how much it will cost an organization to develop one. There are several resources that provide the cost of recovering from an incident and cost/benefit analysis that compare costs of recovery to costs of prevention. These resources are available at the following URLs:¹⁶

- Developing an Effective Incident Handling Cost Analysis Mechanism, by David A. Dittrich; SecurityFocus, June 12, 2002, <http://online.securityfocus.com/infocus/1592>.
- Incident Cost and Analysis Model Project, <http://www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/ICAMP.shtml>.
- Computer Crime and Security Survey from Computer Security Institute (CSI) in partnership with the FBI, 2002, <http://www.gocsi.com/press/20020407.html>
- Computer Crime and Security Survey from Computer Security Institute (CSI) in partnership with the FBI, 2003, <http://www.gocsi.com/forms/fbi/pdf.jhtml>
- 2001 Information Security Industry Survey, <http://www.infosecurimag.com/articles/october01/images/survey.pdf>

Without appropriate resources to maintain the mission of an internal CSIRT, assigning CSIRT functions to existing staff or outsourcing services may be the most viable alternative.

Management Buy-In

For a CSIRT to obtain the necessary resources for its establishment and to succeed, it will require the support and buy-in from senior management. This support can be realized only if senior management understands the mission, goals, and objectives of the CSIRT. Senior management should include the board of directors, president or chief executive officer (CEO), chief financial officer (CFO), director of Information Technology, and the corporate security officer. Senior management should be aware of the overall strategic goals of the CSIRT and understand how CSIRT goals support the business goals and objectives. Senior management should also be apprised of the organizational model for the CSIRT, estimated start-up costs, sustainment costs, and resources required. Senior management's input should be used to refine the vision for the CSIRT.

Staffing and Training

CSIRT staff must be technically educated in hardware, software, and networking basics with a broad understanding of the technologies in use. Of even greater importance, staff must also possess organizational, communication, and interpersonal skills to facilitate interaction and diplomacy with constituents, other teams, vendors, and external organizations. Staff must be able to prioritize work under pressure, making sound decisions where minimal information and direction are given. Based on the impact to the business, a staff member must be dependable, responsible, and reliable. Due to the sensitivity of the information and systems handled, potential staff should go through a stringent interview and background validation to ensure the integrity of the individual. This should include signing CSIRT-specific agreements that address confidentiality, intellectual property, and non-disclosure.

Training is required to give staff members the necessary skill sets to perform their work. It also helps broaden the abilities of the team and keep up-to-date on new technologies and intruder techniques. After new staff members have received the basic skills in the technologies in use, they will need to obtain skills focused on incident handling. At the bottom of Exhibit 8-4 is an example of a list of courses recommended from a Department of Defense (DoD) CSIRT. Organizations not under the DoD will not have access to DoD certifications and courses.

Similar incident handling certification is available from the Carnegie Mellon Software Engineering Institute (SEI), SANS, and CSI. In addition to other security courses, the SEI specifically offers the CERT-Certified Computer

INFORMATION SECURITY ARCHITECTURE

Security Incident Handler Program. This program is for incident handlers, CSIRT managers, system and network administrators with incident handling experience, and incident handling trainers and educators. The program includes four CERT courses designed to provide a breadth and depth of knowledge in incident response:

- Creating a Computer Security Incident Response Team
- Managing Computer Security Incident Response Teams or Fundamentals of Incident Handling
- Advanced Incident Handling for Technical Staff
- Information Security for Technical Staff

This program also requires university or college credits in computer forensics, intrusion detection and analysis, or security audits and assessments.

SANS offers courses on the following CSIRT-related topics:

- Intrusion detection
- Intrusion prevention
- System forensics, investigation, and response
- Cutting-edge hacking techniques
- E-warfare
- SANS Cyber Warrior
- SANS honeypots
- Reverse-engineering malware

The SANS certification has a broader focus targeted at security professionals with a wide range of responsibilities. This certification has five levels and is called the Global Information Assurance Certification (GIAC), as discussed in Chapter 5. The courses offered by the Computer Security Institute (CSI) with a focus on CSIRT functions are:

- Defense against Social Engineering
- Hands-On Hacking
- A Structured Approach to Incident Response

CSI certification also focuses on the security professional in general and is called the Certified Information Security Manager (CISM). Other general security certifications are available from the International Information Systems Security Certification Consortium, Inc. (ISC)² and include the System Security Certified Practitioner (SSCP) and the Certified Information Systems Security Professional (CISSP). These were discussed in depth in Chapter 5. The Web sites for these courses and certifications are listed below:

- <http://www.sei.cmu.edu/>
- <http://www.sans.org>
- <http://www.gocsi.com>
- <http://www.isc2.org>

Policy Development

Policy development is critical for the CSIRT. There are several general security policies that the organization should already have in place even if a functioning CSIRT does not exist. These policies will be essential to the development of the CSIRT. Policies include:

- Code of Conduct Policy
- Information Classification Policy
- Information Dissemination Policy
- Security Policy
- Training Policy

The nature of having to operate and interact with such a diverse set of individuals and groups under stressful and critical situations and with sensitive information requires CSIRT staff to be above reproach in performing their responsibilities. A CSIRT Code of Conduct should address performing one's duties with professionalism. The policy should include such elements as integrity, simplicity, communication, quality, sensitivity, and diplomacy.

The Information Classification Policy standardizes how information is categorized by its level of sensitivity. There are many ways to classify information. Categorizations should be based upon business use. The military has several ways of categorizing information. The more general categories are "Unclassified" and "Classified." Additional categorizations are "Public," "For Official Use Only," "Sensitive," "Secret," and "Top Secret." Specific rules are defined in the Information Classification Policy for how these types of information should be distributed, retained, protected, and destroyed. While "For Official Use Only" information can sit openly on a desk, it is not typically released to the general public and it should be shredded when it becomes obsolete. A CSIRT needs to understand how the organization classifies information and the CSIRT may define its own set of categorizations. For example, anything not "Public" is treated as "Sensitive," and the rules for "Sensitive" information within the CSIRT will be the same as those for the highest level of classification as defined by the organization.

The Information Disclosure, Dissemination, or "Media" Policy defines how information will be disseminated. Security incidences are extremely sensitive and can impact the success of the business. Take the example of a major bank that has had an incident of unauthorized access to its client accounts. When knowledge of the incident becomes public, the bank is going to have a significant loss in clients due to trust, possible negative shareholder activity, and repercussions from its board of directors. The Information Disclosure Policy defines a central point of contact for distributing information to the public or interfacing with the media. Acting proactively to distribute reputable and quality articles or information on incidences can be achieved by establishing a list of media contacts that are

made aware of the procedures for information dissemination within your organization through this policy.

The Security Policy was discussed in depth in Chapter 3. Security procedures must apply to CSIRT members as well and should be an integral part of their operations. This policy includes the physical and logical security of information, systems, and networks, and disaster, recovery, and continuity planning.

The Training Policy should detail the training requirements for users, administrators, and CSIRT members. The CSIRT training requirements were listed in previous paragraphs of this chapter. Establishing a policy for training provides validity to the operation of the CSIRT. Having a policy that is reviewed and approved by management provides the justification for management to provide the necessary resources to follow through and implement an appropriate training plan that enables CSIRT members to perform their duties adequately.

Legal Issues

The CSIRT should operate closely with a legal department to review policies and procedures, provide advice regarding CSIRT operations and practices in relation to laws and regulations, and to assist with litigating incidences or upholding policies and procedures that enact sanctions. Analysis and investigations related to incidences often lead to assets owned by other organizations, especially with incidences that originate outside the organization. Internal CSIRT policies and procedures will most likely not carry much weight on public networks or within other organizations.

Policies and procedures related to CSIRT and security operations should be reviewed by a legal representative to ensure that they are valid and can be upheld in any legal proceedings. This applies to contacts, service agreements, and waivers of responsibility. Waivers are often used to show due diligence when attempting to protect an organization by disclosing such procedures as network monitoring, access, and review of e-mail traffic or data. While many disclaimers may not hold up in court, they can demonstrate the organization's due diligence in protecting its assets.

CSIRTs, security managers, and network and system administrators run into several legal roadblocks with the First and Fourth Amendments of the Bill of Rights. These amendments are specifically designed to protect citizens' rights of free speech and unreasonable search and seizure. This applies to public networks. On private networks, more recent regulation of the First Amendment permits prohibiting employees from such activities as accessing sexually explicit materials, disclosing information regarding facility security, and communications that are prejudicial to good order and discipline when using a private organization's resources as long as policy indicates the prohibition.

There are some limitations as well to the Fourth Amendment, which deals with unreasonable search and seizure. On public networks, individuals have the right to access and view what is openly available and have a right to do so privately. When dealing with government or private organizational networks, systems, and information, that right to privacy is reduced. There are limitations. Network and system administrators and CSIRT members have a mission to attempt to identify problems and to repair and restore systems. In performing that mission, they can view and examine anything that assists them in performing that mission. This includes reviewing an employee's downloads and e-mails while performing the system administrator function. The Fourth Amendment holds firm, however, for criminal investigations. For this reason, network and system administrators and CSIRT members must stop prying into files and seek legal assistance when they believe that a specific individual has broken a regulation or committed a crime. Not doing so could taint evidence of a crime and could also implicate the administrator or CSIRT member in committing his own set of crimes.

CSIRT members should be familiar with several federal laws that help them recognize criminal activity when they see it and to ensure that they do not commit a crime when responding to an incident. Federal laws include, but are not limited to:

- The Privacy Protection Act
- The Electronic Communications Privacy Act of 1986
- The Foreign Intelligence Surveillance Act
- The Computer Fraud and Abuse Act
- The USA Patriot Act of 2001

Chapter 10 provides a discussion of these laws as well as other regulations in much greater detail.

Due to the nature of CSIRT operations, another legal issue that CSIRT members and management must concern themselves with is liability. Liability issues can arise from the following circumstances:

- Lack of information disclosure
- Forgetting about side effects to other organizations or vendors
- Failure to comply with legal reporting and archiving requirements

CSIRTs that do not have direct access to legal advice are operating at a great disadvantage. Making a wrong move or decision can result in the downfall of the CSIRT. It can also invalidate what a CSIRT has gathered as evidence. For this reason it is wise to get law enforcement involved at the beginning of the analysis phase to ensure procedures are conducted within federal guidelines of evidence collection.

Reevaluation of CSIRT Operations

In developing a CSIRT, management must reevaluate CSIRT operations to ensure that the CSIRT mission, goals, and objectives are achieved. Management should evaluate the priorities of the CSIRT to ensure that responses to the most important activities are being met. It will be necessary to revise any policies and procedures as appropriate to meet the real-time challenges placed before the CSIRT. And finally, the services listed in the mission statement should be reevaluated to ensure that they are realistic and achievable. If they prove otherwise, their scope and nature may require modification.

Chapter Summary

This chapter has provided an overview of the operations and services of a corporate CSIRT and the general concepts involved in incident response handling. Incident response handling capabilities of a CSIRT include:

- Recognizing and reporting events and incidences as they are occurring
- Examining what has been reported and reacting quickly to minimize damage (triage)
- Applying known solutions to an intrusion
- Stabilizing the system
- Performing objective analysis of the incident to ensure thorough response, documentation, and to provide lessons learned

The development and management of a corporate CSIRT entails understanding the requirements of the corporation and scoping the CSIRT services to meet the goals and objectives of the organization. It is highly recommended that corporations interested in developing their own CSIRT read available information on lessons learned and understand the issues before embarking on an internal service offering. The CERT/CC also provides well-established CSIRT training programs for CSIRT development, basic incident response handling, and advanced incident response handling. It is also highly recommended that managers delegated with the responsibility of CSIRT development attend seminars and classes to fully comprehend the scope of this security service.

Getting Started

1. Evaluate the functions and services (reactive, proactive, and security quality management services) of a CSIRT being performed within the organization and identify individuals responsible for those functions.
2. Identify what level of these services your organization requires and if these services should be offered on an ad hoc, contract, or formal internal organizational basis.

3. When developing a CSIRT, focus on incident response handling capabilities and artifact handling before moving on to the other reactive services of alerts and warnings, and vulnerability handling. It is likely that vulnerability handling has already been established as a responsibility of the system and network administrators.
4. Develop and document procedures to handle reporting, triage, identification, forensic evidence collection, tracking and tracing, coordination, containment, eradication, recovery, and notification. Train personnel on those procedures.
5. Develop standard reporting forms and be sure they are readily available to employees. Ensure that annual or semi-annual training on the use of these forms is provided to all employees. Training can be held in conjunction with annual security training requirements.
6. Review all systems and system components on the network to gain an understanding of what systems have logging and auditing capability and what information is contained in the log and audit files. Establish procedures to ensure that monitoring is performed on these files and that file sizes are appropriate. Establish a central server for the collection of log and audit files that can be secured.
7. Ensure that all component clocks on the network are time synchronized and time-stamping is utilized to aid the evidence collection and analysis process.

Notes

1. Georgia Killcrece, Klaus-Peter Kassakowski, Robin Ruefle, and Mark Zajicek, *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*, (CMU/SEI-2003-TR-001), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, October 2003. (See Table 1, CSIRT Acronyms and Names, p. 13).
2. Georgia Killcrece, Klaus-Peter Kassakowski, Robin Ruefle, and Mark Zajicek, *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*, (CMU/SEI-2003-TR-001), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, October 2003. (See Table 1, CSIRT Acronyms and Names, p. 12.)
3. Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs) — 2nd edition* (CMU/SEI-2003-HB-002), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003, Table 12, p. 62.
4. Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs) — 2nd edition* (CMU/SEI-2003-HB-002), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003.
5. Georgia Killcrece, Klaus-Peter Kassakowski, Robin Ruefle, and Mark Zajicek, *State of the Practice of Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-TR-001), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, October 2003, p. 65.
6. <http://www.assist.mil> and <http://www.assist.disa.smil.mil>.
7. <http://www.assist.mil> and <http://www.assist.disa.smil.mil>.

INFORMATION SECURITY ARCHITECTURE

8. Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs) — 2nd edition* (CMU/SEI-2003-HB-002), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003. p. 92.
9. Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs) — 2nd edition* (CMU/SEI-2003-HB-002), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003, p. 69.
10. Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs) — 2nd edition* (CMU/SEI-2003-HB-002), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003, pp. 70–73.
11. <http://www.cert.org/csirts/services.html>.
12. Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs) — 2nd edition* (CMU/SEI-2003-HB-002), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003, p. 93.
13. Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs) — 2nd edition* (CMU/SEI-2003-HB-002), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003, p. 94.
14. Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs) — 2nd edition* (CMU/SEI-2003-HB-002), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003, p. 12.
15. Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs) — 2nd edition* (CMU/SEI-2003-HB-002), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003, p. 190.
16. http://www.cert.org/csirts/csirt_faq.html#10.

Chapter 9

Conclusion

There are many reasons that an Information Security Architecture has become critical to the operation of those organizations dependent upon their computing environment to succeed. The increasing growth and use of the Internet to conduct business has brought about great changes in the computing environment for businesses, organizations, and individuals. The Internet, e-mail, and networks have increased communications and commerce channels between companies and their employees, clients, vendors, business partners, and even their competitors. While much more can be accomplished by empowering users through the use of advanced technologies, the risks to all have been greatly increased as well by these new technologically enriched environments.

It is becoming rare for employees to not use PCs in order to perform their daily responsibilities. It is becoming even more rare that individuals and employees do not have access to e-mail and the Internet or, for that matter, a personal Web site. Networks, Internet, new software applications, software targeted at hobbies, and personal productivity tools have given just about every profession and every individual a reason to become computer literate. Computer literacy and the preponderance of computer users have provided the link and the know-how for those individuals with other than positive productivity and efficiency in mind to exploit networks and computer resources for personal gain and resulting in a negative impact to the organization.

Internal to an organization, users who are computer-savvy can make their way through the network electronically and exploit vulnerabilities to gain access to applications and confidential information. Individuals may have a vengeance against an employer or an employee and seek to cause damage, wreak havoc in computer systems and components, or expose a company's secrets. On the other hand, computer users may unknowingly execute or fail to execute procedures that result in damage, exposure, or embarrassment to the organization. Computer viruses are a good example of this. An employee who is searching the Internet for company-related information may accidentally download a file containing a virus that brings down the entire system and causes significant loss to the organization.

INFORMATION SECURITY ARCHITECTURE

Interconnectivity via intranets, internets, extranets, and the Internet have provided those external to the organization an opportunity to gain access to an organization's internal operating environment. Hackers or those with ill intentions can exploit software, components, network flaws, or configurations with weak security designs to gain illegal and unauthorized access to confidential resources resulting in significant losses to the organization.

There are so many positive reasons to develop a computing environment that takes advantage of all that technology has to offer. There are many risks in doing so without looking at both the benefits and the threats. The Information Security Architecture is designed to protect the investments made in technology and to protect the information and computing resources of the organization so that the organizational goals and objectives can be met.

An organization must understand the security life cycle and determine where the organization is in that life cycle. The security life cycle consists of assessment, development, implementation, and maintenance of the security components of the organization. The security structure within an organization must include a team of individuals, as discussed in Chapters 2 and 3, that develop the Information Security Architecture and ensure that the security life cycle is active and effective within the organization. Assessment includes looking at all of the processing components that are critical to continued operations and determining the vulnerabilities and level of risk related to each of those components. Once the level of risk has been determined, resources can be applied to protect those processes and components that pose the most risk of loss to the organization. Assessments can be in the form of a security baseline review as discussed in Chapter 4, where no previous assessment has been performed. Assessments can also be in the form of a systems audit related to external or internal financial reviews of the organization as discussed in Chapter 6.

The second step of the security life cycle consists of developing mechanisms that reduce risk to an acceptable level within the processing environment. Security policies need to be developed to bring about awareness of the proper operating procedures within the organization. Security standards need to be developed to make security operations more efficient. Security procedures provide the step-by-step instructions for executing those protective mechanisms. These components of the ISA were discussed in Chapter 3. Once these security policies, standards, and procedures are written and approved, they must be implemented correctly.

Implementation of the Information Security Architecture consists of defining the security responsibilities of each individual within the organization and communicating those responsibilities to each of those individuals. Implementation includes:

- Providing the necessary resources such as hiring appropriate personnel to be able to execute the responsibilities that have been defined
- Providing the resources to train personnel to perform those responsibilities effectively
- Developing weekly, monthly, and quarterly meetings to discuss security issues and concerns; and make progress with the ISA as well as understanding where in the security life cycle the organization stands
- Enforcing the policies, standards, and procedures that have been developed
- Educating all users throughout the organization on security through security awareness training
- Purchasing and installation of hardware and software tools to effectively assess, monitor, and alert the security teams of potential security breaches and issues
- Providing the necessary financial, personnel, and time resources to improve the organization's processing environment by reducing risk and addressing the security concerns that have been discovered in the assessment phase

Once the organization has done all of these things and the security infrastructure appears to be functioning effectively, it enters the maintenance phase of the security life cycle. The maintenance phase consists of evaluating whether the security infrastructure is really effective. The ISA must have a defined mechanism for measuring whether the policies, standards, and procedures are being followed, whether the controls of the organization will in fact reduce risk to the organization, and whether improvements need to be made to further reduce risk. This mechanism is called compliance and is executed through audits and independent assessments.

Change in today's computing environments is perpetual. New components are being added to the processing environment, new access rules are being defined, users are added and deleted to the system, new ways of doing business with the most recent technology are being discovered, security holes and vulnerabilities are exploited daily, and viruses are developed and disseminated on nearly a weekly basis. In light of all of this, an effective ISA today, may not be as effective tomorrow given the dynamics of the processing environment and the rate of change in business. Maintaining the ISA needs to be in response to the changes that are applied to the organization and the processing environment. The security life cycle begins again with the assessment phase and the evaluation of those changes, their effects on the organization, and the steps that need to be developed and implemented to respond to those changes.

Security in the organization can be manageable and effective with an understanding of the business and computing environment, some basic organization skills, and the ability to gain understanding and support from

INFORMATION SECURITY ARCHITECTURE

executive-level management. This book has attempted to guide the reader through the steps necessary to effectively assess and understand an organization and to apply a step-by-step approach to building the security infrastructure in a building-block approach. This book has also sought to provide an understanding of the pitfalls that have caused other ISA projects to falter and fail. Armed with this understanding, one will be able to avoid the most common pitfalls that derail security within the organization.

Security software and methods are beginning to mature. Open architectures have forced the security community to integrate security products with more and more operating systems and processing architectures to meet the challenges of balancing resources and reducing the number of security products necessary to implement. Understanding the current security products and technologies already available and under development will help an organization make better choices related to its direction and requirements regarding security implementation efforts.

Implementing new technologies comes with a responsibility to understand not only the technology's return on investment to the organization, but also the risks and vulnerabilities related to that technology. This author's goal has been to provide a relatively easy methodology that takes the fear out of embracing new technology by balancing implementation efforts in a reduced risk environment.

Appendix A-1

Information Security Policy

STARCROSS, INC.

INFORMATION SECURITY POLICY

Author(s):	Security Team	Policy Effective Date	July 31, 2004
Approval Authority:	Executive Committee	Last Revised	July 31, 2004
	Policy for Security	Policy Review Date	January 31, 2005

INTRODUCTION

The widespread implementation and use of networks and a distributed client/server processing environment is accompanied by new risks and exposures. Networks provide us with greater flexibility for accessing and sharing information and resources and for performing processing at the desktop. These advantages to networking also increase the exposure of sensitive information and make it necessary to implement control strategies to maintain information confidentiality, integrity, and availability.

This document contains a high-level statement of Starcross Inc.'s information security intentions, expectations, and objectives, and the necessary implementation strategy for their attainment. This policy is the foundation for all information security activities, including enterprise security architecture development and implementation. It focuses not only on the technology for the storage, processing, and transmission of LAN-based information, but also on administrative and operational practices for the protection of all information, data, files, and processing resources owned by Starcross. All information, data, applications, networks, and equipment (including PCs and printers) are the property of Starcross and is provided to its employees so that they can conduct their job responsibilities effectively. These assets should be treated with privacy and confidentiality when conducting business and should not be made available or accessible to anyone outside the enterprise without specific written permission of the Chief Information Officer.

This policy is the property of Starcross. It was developed under the direction of the Chief Information Officer by the Security Team comprised

INFORMATION SECURITY ARCHITECTURE

of network, administrative, and information systems representatives. It is intended for distribution to all employees and users of information systems at Starcross locations.

Due to the sensitive nature of the information contained within the security policy, standards, and procedures, all distribution of these documents must be based on sound business requirements and be approved by the Chief Information Officer.

Table of Contents

1.0	Policy	245
1.1	Information Security Policy	245
1.2	Policy Objectives	246
1.2.1	Security Management	246
1.2.2	Confidentiality	246
1.2.3	Integrity	247
1.2.4	Availability	247
1.2.5	Non-Repudiation	247
1.2.6	Authentication	247
1.3	Policy Scope and Responsibilities	247
1.3.1	Policy Scope	247
1.3.2	Security Officer	248
1.3.3	Security Coordinators	248
1.3.4	Security Team	249
1.3.5	Executive Committee for Security	249
1.3.6	Help Desk	249
1.3.7	Departmental Management	250
1.3.8	Application Coordinators	250
1.3.9	Human Resources Department	250
1.3.10	Internal Audit	250
1.3.11	Information Users	251
1.4	Implementation	251
1.4.1	Information Resources	251
1.4.2	System and Information Ownership	252
1.4.3	Access to Systems and Information	252
1.4.4	Security Monitoring and Enforcement	254
1.4.5	Security Awareness Program	254
1.4.6	Computer Security Incident Response Team (CSIRT)	255
1.4.7	Disaster Recovery / Business Continuity Planning ...	255
1.5	Controls	255
1.5.1	Risk Assessment	255
1.5.2	Corporate Policies	256
1.5.3	Departmental Procedures and Guidelines	256
1.5.4	Starcross Policies and Procedures Manual	256
1.5.5	Starcross Security Standards and Procedures Manual	257

1.0 POLICY

1.1 Information Security Policy

1.1.1 Information Assets. Starcross information and information processing infrastructure are vital assets requiring protection commensurate with their value. Organizational information, applications, systems, and networks must be actively managed to ensure security, confidentiality, integrity, and availability.

1.1.2 Accountability. The administrative and departmental computing environments will maintain consistent standards for establishing the accountability and authenticity of system users, which will be compatible with internal accounting control standards prescribed by Starcross, Inc.

These environments will develop unique standards for protecting information, applications, systems, and network resources contained within these environments that will be commensurate with fulfilling the mission of Starcross and maintaining the integrity of those critical resources.

To maintain accountability for system access, we will implement the following:

- All individuals with access to the systems will use a user ID that has been specifically assigned to that individual. Sharing of user IDs is prohibited except in specific, approved situations. Written justification for such an ID is required and approval for use will be granted only by senior management.
- All individuals with network, system, and application user IDs will retain a confidential password that will be used to authenticate the identity of the individual. Intentional disclosure or sharing of passwords is prohibited. To meet the needs of some applications, certain terminals can utilize a location or station password, with strictly limited access to applications. User IDs will be required on all documents generated or modified.

1.1.3 Information Access. All access to information is to be authorized by responsible management, with access granted or revoked based on business requirements only. Access to administrative data will be granted to Starcross employees only. Individuals outside of Starcross can be authorized access to Starcross data only if that authorization is granted by the appropriate Department Manager and the Chief Information Officer.

Access and update capabilities/restrictions will apply to all Starcross administrative, departmental, and operational data, stored on the administrative, departmental, and operational systems computing facilities. Security measures apply to all systems developed and/or maintained by Starcross locations, departments, organizations, affiliates, outside vendors, or contractors.

INFORMATION SECURITY ARCHITECTURE

The appropriate Department Manager and the System Administrator are responsible for authorizing access to systems and information, verifying information integrity, and controlling extracted information. Management is responsible for developing secure processing systems and operating these systems in a controlled environment. Employees are required to comply with management's direction for the use and protection of information technology processing systems and information. Employees must be kept aware of the importance of information security. All managers and employees are required to act with urgency and diligence to fulfill these requirements.

Risks must be evaluated to determine the optimum level of control required for each type of information technology system. Adequate controls are to be included to ensure that information security, confidentiality, integrity, and availability are achieved.

1.1.4 Violation of Policy. Violation of this policy should be brought to the immediate attention of the Security Officer. Violations should be reported to Bill Gernsey. Instances of known or suspected employee infidelities should be reported to the Security Officer and the Chief Information Officer. The Security Officer will work with Department Managers, LAN Administrators, and the Security Team to ensure that the problem is resolved and to address necessary steps to eliminate future violations. An escalation process will define the course of action for all violations consistent with the severity of the violation.

Detailed security standards and procedures are documented in the Starcross Security Standards and Procedures Manual (SS&PM).

Starcross reserves the right to discipline, terminate, suspend, or prosecute, at its discretion, individuals who violate the information Security Policy.

1.2 Policy Objectives

1.2.1 Security Management. The security of corporate information, applications, systems, and networks is fundamental to the continued success of Starcross. Security management seeks to establish controls and measures to minimize the risk of loss of information and system resources, corruption of data, disruption of access to the data, and unauthorized disclosure of information. Security management is achieved through effective policies, standards, and procedures that will ensure the confidentiality, integrity, and availability of Starcross information, applications, systems, and networks for authorized users.

1.2.2 Confidentiality. Confidentiality relates to the protection of information from unauthorized access regardless of where it resides or how it is stored. Information that is sensitive or proprietary needs to be protected to a higher level than other information. Policies are in place to identify what information is confidential and the period of time it should remain

confidential. The SS&PM provides a framework for classifying the confidentiality of data according to its characteristics and indicates associated security requirements for each confidentiality ranking.

1.2.3 Integrity. Integrity is the protection of information, applications, systems, and networks from intentional, unauthorized, or accidental changes. It is also important to protect the processes or programs used to manipulate data. Information should be presented to information owners and users in an accurate, complete, and timely manner. Key to achieving integrity is identification and authentication of all users accessing information, applications, systems, and networks through the use of manual and automated checks. Employees must not take any action that could compromise the integrity of the information, application, system, or network.

1.2.4 Availability. Availability is the assurance that Starcross information and resources are accessible by authorized users as needed. There are two issues relative to availability: denial of services caused by a lack of security controls (e.g., destruction of data or equipment, computer virus), and loss of services from information resources due to natural disasters (e.g., storms, floods, fires). Denial of services is addressed as a part of security management and will be discussed later in this document. Loss of services is addressed as part of the Business Continuation Planning process. The SS&PM provides a framework for classifying the availability of data according to its characteristics and indicates associated security requirements for each availability ranking.

1.2.5 Non-Repudiation. Non-repudiation requires proof of delivery and assurance of source. Neither sender nor the receiver of information is able to deny the transmission or its receipt. Digitally signed messages using public and private keys provide the non-repudiation security service for digital computer messages and transactions.

1.2.6 Authentication. Authentication requires that the origin of a message be correctly identified with assurance that it is not a false or forged identity. Passwords are used to authenticate a user based upon the fact that only the user should know the password. Strong passwords will be used and must contain a number of rules such as combinations of letters and numbers with combinations of upper and lower cases. One-time passwords will also be implemented for high-risk applications as well as encryption to provide the authentication security service to identify the origin of messages.

1.3 Policy Scope and Responsibilities

1.3.1 Policy Scope. This policy applies to all employees, vendors, contractors, and consultants who create, distribute, access, or manage information by means of Starcross's information technology systems including

INFORMATION SECURITY ARCHITECTURE

personal, department, or corporate computers, networks, and communication services by which they are connected. It equally applies to individuals and enterprises, who by nature of their relationship to Starcross, are entrusted with confidential or sensitive information. This policy addresses all aspects of information security and continuity from initial design of a system through implementation and operation. It also addresses any device used to store, process, or communicate Starcross proprietary or other protected information.

It is the intent of Starcross management to provide direction and an environment that facilitates the communication and use of information within the bounds of sound business practices, and the legal or regulatory restrictions that apply. Security policies, standards, procedures, and business continuation plans have been developed to provide consistency in implementing controls. These define protection requirements or provide guidance to management responsible for implementing controls within their business functions. It is the intent of this policy to facilitate the exchange of information and computing resources while balancing the need for protecting information with the cost of implementation.

1.3.2 Security Officer. The Security Officer of Starcross has overall responsibility for information security matters. These responsibilities are to:

- Ensure appropriate user access and authentication controls are in place.
- Ensure that the documented security policies, standards, and procedures are reviewed, updated, and maintained periodically by appropriate individuals.
- Evaluate security exposures, misuse, or non-compliance situations and ensure implementation of security controls to address those incidences.
- Ensure that all department Security Coordinators understand and execute their security responsibilities in accordance with related policies, standards, and procedures.
- Organize and conduct periodic Security Team meetings.
- Develop and implement the Security Awareness Program with assistance from the Security Team members.

1.3.3 Security Coordinators. Security Coordinators will be assigned within each site or department. The Coordinator's primary responsibility is to ensure that appropriate user access within the scope of their business function is maintained. Additional responsibilities include:

- Ensure that Application Access Forms are initiated for existing and new users within the respective departmental area.

- Ensure that access is modified or deleted when employees and non-employees operating within their business function or site are transferred or terminated.
- Conduct user security awareness within their departmental function.
- Ensure that the Starcross Confidentiality Agreement and Exit Interview Form are signed by all users operating within their department or area of responsibility.
- Actively participate as a member of the Security Team.
- Coordinate with the Security Officer on all security-related matters.

1.3.4 Security Team. The Security Team is comprised of the Security Officer, Security Coordinators, network, applications, and Internal Audit representatives within Starcross. This team is responsible for communicating to management the risk control strategies that are being considered for implementation across sites and to report management's concerns about these protection measures. Specific functions of the team together with operating management are to:

- Represent particular security and business continuation issues and concerns within each Starcross site.
- Identify risks within their area of concentration and ensure that appropriate controls are implemented to address these risks.
- Recommend, review, and approve all security policies, standards, and procedures that will be implemented across sites.
- Develop and implement an Information Security Awareness Program for all information technology administrators, development personnel, users, and their management, and administer the implementation of this program within their area.

1.3.5 Executive Committee for Security. The Executive Committee for Security is comprised of director-level management responsible for reviewing all security plans relating to the protection of Starcross systems and electronic information assets. In this role, the Executive Committee for Security is responsible for reviewing the policy and for ensuring that all implementation plans, procedures, and standards are consistent with the overall risk management and protection expectations of Starcross's senior management. When appropriate, the Executive Committee for Security will forward recommendations for approval to the Board of Directors.

1.3.6 Help Desk. The Help Desk will maintain the Security Policy, and the Security Standards & Procedures Manual (SS&PM) online. The Help Desk will be responsible for answering security-related questions in accordance with policy, standards, and procedures and for directing security-related issues to the appropriate department management in accordance with Security Incident Escalation Procedures as defined in the SS&PM. Help

INFORMATION SECURITY ARCHITECTURE

Desk will also provide password management assistance to include security awareness to users in strengthening and protecting passwords.

1.3.7 Departmental Management. Department Management in this document refers to Starcross managers who are responsible for functional business areas. Reference to Departmental Management generally means the head or a designated person who has the responsibility and authority to act on behalf of senior management. This person is also considered the owner of the information. Departmental Management is responsible for establishing the overall security strategy for department information. This includes determining the security classification of information owned by the department. Classifications will indicate the level of sensitivity and availability required for the information. In addition, Department Management is responsible for authorizing the level of access to information within each respective department function.

1.3.8 Application Coordinators. Application Coordinators are jointly established by department and systems management and report directly to these managers. These Coordinators are responsible for assisting the Department Manager in implementing and managing information technology security policies, procedures, standards, and departmental guidelines within their functional area. The Coordinator serves as the principal liaison between their department and the Network Administrators.

1.3.9 Human Resources Department. Human Resources is responsible for managing and coordinating hiring, termination, and disciplinary practices within Starcross. Human Resources and Departmental Management are responsible for providing timely information to the enterprise LAN manager about employee termination or transfers so that appropriate steps can be taken to revoke or change access to systems and information. Human Resources will also ensure that new hires will be given the opportunity to read both the Security Policy and the Information Security Policy Acknowledgment Form and sign the Information Security Policy Acknowledgment Form. In addition, Human Resources will ensure that the Exit Interview and Reaffirmation of Confidentiality Obligations is read and signed by all employees leaving the company.

1.3.10 Internal Audit. The Internal Audit function is performed by the Internal Audit Department, which is responsible for periodically reporting on the effectiveness of information technology security policies, standards, and procedures and evaluating the appropriateness of risk management techniques utilized by Starcross. Annually, in cooperation with Starcross management, Internal Audit identifies departments, business functions, systems, or applications to be reviewed, and conducts inquiries and tests to determine the level of risk, as well as the effectiveness of controls and compliance with policies, standards, and procedures established

by Starcross management. Internal Audit is also responsible for ensuring compliance with software licensing agreements. Internal Audit reports to management their results and, where applicable, recommendations for improving risk management capabilities as well as any instances where policies, procedures, and standards are not effectively implemented. Internal Audit provides written reports to Halford and Associates, Starcross's external auditors, and the Chief Financial Officer.

1.3.11 Information Users. Information users include all employees of Starcross who access or receive information produced, stored, or communicated by Starcross's information technology systems. Information users also include all individuals, who by nature of their relationship with Starcross (e.g., contractors, vendors, service providers, consultants, etc.) are entrusted with sensitive or confidential information. Information users are responsible for compliance with the Information Security Policy and individual standards and procedures contained within the Security Standards and Procedures Manual.

Noncompliance to the Security Policies and Standards will be investigated and disciplinary actions will be administered by the appropriate immediate manager where the infraction has occurred. Human Resources will be involved as required. Disciplinary actions can range from a verbal warning to employment termination, suspension, or prosecution.

Information users who are not Starcross employees are also bound by the signed agreement between Starcross and the individual or company that addresses non-disclosure of Starcross information.

1.4 Implementation

1.4.1 Information Resources. Information resources including computer software and support systems should be protected appropriately to maintain the sensitivity and critical nature of information that is processed, stored, or communicated. Information systems should be protected in such a manner to ensure that unauthorized persons are not able to directly access the device and either cause physical damage or modify internal components that could affect the results of computing or other processes. Environmental and security controls should be appropriate for the level of risk. An assessment that balances risk with the cost of implementing the control should be completed when determining what security and environmental controls are appropriate.

Information resources should be classified by the designated data owner using the risk assessment guidelines described in the SS&PM. Information assets are classified to provide a means of communicating the level of protection to be provided. Information security requirements will vary with the sensitivity and level of importance of the information or the systems associated with that information.

INFORMATION SECURITY ARCHITECTURE

Users are responsible for adhering to copyright, patent laws, and license agreements for intellectual property. Violations of authorial integrity, which may be grounds for sanction, include plagiarism, invasion of privacy, unauthorized access, trade secrets, and copyright violations.

Communication facilities and equipment should be protected from unauthorized modification and tampering to ensure that messages in transit are not modified or received by unintended parties or that communication services are not interrupted. Communication facilities can include all equipment rooms and wiring closets and may include facilities and resources provided by third-party service providers.

Questions concerning the appropriateness of physical and environmental controls should be addressed to the Security Officer.

1.4.2 System and Information Ownership. Starcross is the owner of all information, applications, systems, and software that is developed, used, or distributed to employees or designated representatives of entities operating as business partners. Although Starcross maintains the ultimate ownership responsibility, certain managers are responsible for executing this responsibility.

Systems and information owners are responsible for identifying and managing risks relating to the security, integrity, and continuity of information, and for the business processes and system functions that create, modify, delete, or use this information. They are responsible for assessing the level of risk to Starcross for providing access to information, as well as for determining the impact to the organization if information, business processes, or system functions were not available or if they are misused.

The level of security, integrity, and continuity risk needs to be communicated by the owner to individuals or groups responsible for implementing Starcross security and continuity controls. Business process integrity controls as well as departmental security and continuity measures may need to be implemented by owners to support Starcross protection plans and procedures. Local sites will be responsible for security on their portion of applications, systems, and networks.

Periodically, the Data Owner and the Security Officer will review the current set of access and update capabilities granted to each individual on the system in order to ensure that the appropriate level of access has been granted and that no changes are necessary. Data Owners are indicated in Appendix A of the *Security Standards and Procedures Manual*.

1.4.3 Access to Systems and Information. All access to information and systems is provided based on business need. Information owners, as part of their management responsibility, are required to review all requests for

access to information or systems, and to verify that such access meets a legitimate business need. Approval for access needs must be communicated to the Network Administrator or the department's Security Coordinator as required for implementation.

An Application Access Request Form will be filled out by the user's Departmental Manager. This form will indicate the files and applications that the user should be permitted to access. The Application Access Request Form will be signed by (1) the Departmental Manager, and (2) the Application/Resource Coordinator. The Information Security Policy Acknowledgment Form will be used to acknowledge that each user has read the Information Security Policy and understands the responsibilities in connection with the policy and the consequences of a policy infraction. Examples of the above described forms are located in SS&PM. These completed forms will be retained by the Security Officer.

Access requests for information between departments must meet the same test of business need. When making the decision to either grant or deny access, the owner should consider the benefits to Starcross for granting access, the type of access that is required, and the business risk associated with such access.

Access to certain sensitive information needs to be restricted. Owners may require that information provided to another department is not distributed to other groups without prior approval. Owners may also designate a retention period during which the information or access may be authorized and after which all access is to be revoked. Owners must approve or deny all access requests.

When approval for outside access to Starcross information is granted, detailed instructions must be provided to the recipient notifying them of any security requirements, including the need to maintain the confidentiality of the information, requirements for distribution of the information within their organization, and procedures for destruction or return of the information following the period of access. All non-employees will sign a non-disclosure agreement. More details can be found in SS&PM.

Human Resources will immediately notify the Managers of Information Services of all employee terminations via e-mail. A monthly report detailing employee terminations/resignations will be sent from Human Resources to the Manager of Information Services to confirm the deletion of User IDs. This list will indicate the employees whose LAN and application user IDs should have been removed from the system upon initial notification. The Manager of Information Services will notify the LAN and Application Coordinators who will upon notification, disable the user IDs immediately. A Coordinator will be assigned to ensure that all contractor, vendor, and consultant user IDs are properly disabled upon leaving the company.

INFORMATION SECURITY ARCHITECTURE

When a Department Manager is notified of an employee termination/resignation, they should review the disposition of the user's data and files residing on the network or application directories with the user prior to separation from Starcross. The Manager will notify the LAN and Application Coordinator in writing of those files to be transferred or destroyed. Disposition of any files will follow the guidelines defined by the Documentation Retention Program.

1.4.4 Security Monitoring and Enforcement. It is the responsibility of both Network and Application Coordinators to implement appropriate measures to detect attempts to compromise the security or integrity of information or information technology systems. When implementing monitoring capabilities, consideration should be given as to what situations are to be monitored based on the extent of risk, the most effective means for monitoring security activities, the resources available for monitoring, and system constraints that limit the ability to monitor security events. If appropriate measures are not available within a system environment to effectively monitor security events, additional software should be installed or additional controls to mitigate security risks should be implemented.

When activity occurs that is in conflict with security policies and standards, Application Coordinators or Network Administrators should take the appropriate steps to enforce desired security practices. The steps involved range from training of the users, revoking access, altering security parameters and possibly disciplinary actions.

Due to the likelihood of damage and destruction of information resulting from malicious code, including viruses, detection capabilities must include virus detection software within the local area network environment, as well as on systems that are at high risk for infection.

The facts surrounding an intrusion, infection, or system compromise must be documented, reported to the Security Officer, and include the circumstances that led to the discovery of the incident, actions which were immediately taken, the names of persons involved in investigating the incident, and detailed observations about what transpired, what damage was caused, and what systems or files were compromised.

Starcross will enforce and support the Information Security Policy at its discretion by responding to business ethics violations and employee/non-employee infidelities (known or suspected) through disciplinary action, termination, suspension, or prosecution.

1.4.5. Security Awareness Program. It is the responsibility of management to ensure that all users of information understand how to protect company assets, including information and information resources and comply with security policies, standards, and procedures. Supervisors and

managers must ensure that persons working within their department understand general information security requirements and that they are sufficiently knowledgeable about the information technology security policies, standards, and procedures to recognize the need for protecting information and the requirements for which they are specifically responsible.

The Security Officer with assistance from the Security Team is responsible for developing and implementing an information security awareness program that supports employee awareness. Managers and supervisors need to be aware of user performance in this area, encourage good security practices, and address inappropriate behavior. Application Coordinators can assist in implementing specific awareness programs.

1.4.6 Computer Security Incident Response Team (CSIRT). A Computer Security Incident Response Team (CSIRT) will be identified along with appropriate procedures to react defensively to intrusion and destruction. The Security Officer in conjunction with the Security Team will develop a plan for cyber-defense that includes procedures for incident handling. At a minimum, the CERT will be responsible for identification, containment, eradication, and recovery of all cyber-related incidences.

1.4.7. Disaster Recovery/Business Continuity Planning. It is the responsibility of management to ensure that advanced planning and preparation is performed to minimize loss, reduce impact, and ensure continuity of the organization's functions and revenue stream. A Disaster Recovery/Business Continuity Plan (DRP/BCP) will be developed and tested for effectiveness. At a minimum, the DRP/BCP will include pre-planning risk control, crisis management, and business recovery.

1.5 Controls

1.5.1 Risk Assessment. Risk assessment involves identifying the sensitivity and criticality of information and the consequences to Starcross if information is disclosed, modified, or destroyed. Risk assessment techniques can include formal methods of determining the financial and operational impact of a security incident as well as less formal assessment techniques. A risk assessment process should include the following elements:

- A determination of the information assets that need to be protected
- Evaluation of the sensitivity of the information and the consequences if information is disclosed
- Evaluation of the criticality of information and the consequences to business processes if information and information processing systems are not available
- A determination by management of the extent of risk that will be accepted, mitigated, or transferred

INFORMATION SECURITY ARCHITECTURE

- Development of a risk control strategy
- Determination of compliance with regulatory information classifications

It is the responsibility of management to understand the level of risk to Starcross relating to the confidentiality, integrity, and availability of information and to the controls necessary to effectively mitigate this risk. Risk control measures should address not only the information but the processes that are used to create, modify, report, or distribute information, and the environments under which these processes exist. This process should also incorporate the classification of data/information in accordance with the Starcross SS&PM into one of the following categories:

- Confidential
- Starcross Business Use Only
- Public
- Indefinite
- Medium-term
- Long-term
- Critical

The SS&PM provides a framework for classifying the confidentiality, integrity, and availability rankings for data and the necessary security requirements for each classification.

1.5.2 Corporate Policies. These policies will not conflict with any policies established by Starcross. Although there may be some areas where practices differ, the corporate policy will prevail. Exceptions will be on a case-by-case basis and must be approved by the Executive Committee for Security.

1.5.3 Departmental Procedures and Guidelines. Each department should develop and maintain additional departmental procedures and guidelines that support the overall intent of the Information Security Policy, if necessary to meet special situations. The procedures and guidelines should be specific to the business unit's applications and the security required. Departmental Management is responsible for ensuring that appropriate personnel within the department are familiar with the procedures and guidelines. It should be understood by departmental personnel and particularly the Application Coordinator that their jobs are to be performed in a way that complies with the standards, procedures, and guidelines.

1.5.4 Starcross Policies and Procedures Manual. The Starcross Policies and Procedures Manual provides the general framework for tasks performed in the Information Systems Department. This document defines the methodology for any system and application development.

1.5.5 Starcross Security Standards and Procedures Manual. The *Starcross Security Standards and Procedures Manual* (SS&PM) documents detailed methods for achieving the security objectives stated in this policy. This manual along with the Information Security Policy helps to define the framework for Starcross's Information Security strategy, architecture, and implementation. It focuses not only on the technology for the storage, processing, and transmission of LAN-based information, but also on administrative and operational practices for its protection in all of its forms both inside and outside of Starcross. This document should be referenced to gain a general understanding of Starcross' approach to security.

Appendix A-2

Information Security Policy Acknowledg- ment Form

STARCROSS, INC.

INFORMATION SECURITY POLICY

ACKNOWLEDGMENT FORM

Author(s):	Security Team	Policy Effective Date	July 31, 2004
Approval Authority:	Executive Committee	Policy Last Revised	July 31, 2004
	for Security	Policy Review Date	January 31, 2004

INFORMATION RESOURCE SECURITY

Information Security is the protection of company data, applications, systems, and network resources from accidental or deliberate misuse through unauthorized disclosure, alteration, or destruction.

Information resources include:

1. Printed or written communications and documentation, such as reports, letters, and memos
2. Online screen transactions
3. Software applications
4. Dataset files and databases residing on any media, such as tape, disk, diskettes, microfilm, and microfiche
5. Processing systems to include servers, PCs, workstations, and printers
6. Network resources

It is every user's responsibility to guard against unauthorized use, destruction, or disclosure of these assets. Every user is responsible for reasonable protection of company information and information resources.

INFORMATION SECURITY ARCHITECTURE

Starcross stores, processes, and disseminates large amounts of critical information. Loss, damage, or disclosure of information, applications, systems, or network resources could result in a significant operational or financial loss to the enterprise. It is imperative to insure the integrity, accuracy, availability, and confidentiality of these resources through the use of effective security controls.

USER RESPONSIBILITIES

Each user of Starcross computer systems is responsible for safeguarding the confidentiality and integrity of resources to which he or she has access. This acknowledgment form and the Starcross Information Security Policy applies to all users of the Starcross computer systems, including employees, clients, contractors, and other individuals who have been granted access authority to Starcross computer systems.

If you have a User ID, you are responsible for the confidentiality of the password, and for any action performed with your User ID.

The following guidelines will be adhered to:

1. Your User ID and password are yours; do not loan it out or share it with others. You are personally accountable for all actions that occur under your User ID.
2. Select an alphanumeric password that has both letters and numbers and would not be easily "guessed." Passphrases are the most acceptable, in which a phrase is used in combination with numbers. Do not use repeating characters. Do not use obvious passwords such as your name, your spouse's, children's, or pet's names, days of the week, names of months, your User ID, birthday, phone, or social security number. Make sure your password is a minimum of eight characters in length and it is changed a minimum of every 60 days.
3. Memorize your password instead of writing it down, and do not store it in programmable function keys.
4. Log out or lock your terminal when leaving it, even for a short period of time. Be sure and log out when you leave for lunch.
5. Keep documents, diskettes, and copies of files containing sensitive data in a secure cabinet, desk, or room, and dispose of them properly when no longer needed. Reformat reusable diskettes containing sensitive data before releasing them for reuse.
6. Ensure that your data and transactions are protected against unauthorized use.
7. If you think your User ID and password have been compromised in any way, immediately change your password and notify your supervisor or the Security Coordinator for your business area.

Information Security Policy Acknowledgment Form

8. Report all suspicious activity, breaches in security, and practices not conducive to good data security to your supervisor or the Security Coordinator for your business function.
9. Protect the confidentiality of sensitive data when viewing it online.
10. Company computer resources are to be used for company business only. Use for anything other than that for which you are authorized is considered misuse.
11. Computer users should take precautions to prevent the introduction of software viruses into their PCs. Games, files downloaded from bulletin boards and the Internet, and software brought from home are not authorized and increase the risk of loss due to viruses on the network.

SECURITY POLICY ACKNOWLEDGMENT

Signing this form constitutes acknowledgment by you of your responsibility to guard against unauthorized use or disclosure of company resources or information, and agreement that you will comply with all of the security policies and rules listed in this acknowledgment form and with the Information Security Policy.

Starcross reserves the right to monitor e-mail, voice mail, and processing systems activity, transactions, and files to prevent abuse, misuse, and to maintain effective operations of these systems. Starcross reserves the right to monitor these systems for any other legitimate business reason.

I have read and understand the Starcross Information Security Policy and Acknowledgment Form as presented above.

Signature

Date

(Printed Name)

Social Security Number

Appendix A-3

Network Computing Policy

This organization is responsible for securing its network and computing systems in a reasonable and economically feasible degree against unauthorized access and/or abuse, while making them accessible for authorized and legitimate users. This responsibility includes informing users of expected standards of conduct and the punitive measures for not adhering to them. Any attempt to violate the provisions of this policy will result in disciplinary action in the form of temporary revocation of user accounts, regardless of the success or failure of the attempt. Permanent revocations can result from disciplinary actions taken by a panel judiciary board called upon to investigate network abuses.

The users of the network are responsible for respecting and adhering to local, state, federal, and international laws. Any attempt to break those laws through the use of the network may result in litigation against the offender by the proper authorities. If such an event should occur, this organization will fully comply with the authorities to provide any information necessary for the litigation process.

SECTION 1: GENERAL COMPUTING POLICY

Once a user receives a User ID to be used to access the network and computer systems on that network, they are solely responsible for all actions taken while using that User ID. Therefore:

- 1.1 Applying for a User ID under false pretenses is a punishable disciplinary offense.
- 1.2 Sharing your User ID with any other person is prohibited. In the result that you do share your User ID with another person, you will be solely responsible for the actions that other person appropriated.
- 1.3 Deletion, examination, copying, or modification of files or data belonging to other users without their prior consent is prohibited.
- 1.4 Attempts to evade or change resource quotas are prohibited.

INFORMATION SECURITY ARCHITECTURE

- 1.5 Continued impedance of other users through mass consumption of system resources, after receipt of a request to cease such activity, is prohibited.
- 1.6 Use of facilities or services for commercial purposes is prohibited.
- 1.7 Any unauthorized, deliberate action that damages or disrupts a computing system, alters its normal performance, or causes it to malfunction is a violation, regardless of system location or time duration.

SECTION 2: ELECTRONIC MAIL POLICY

Whenever you send electronic mail, your name and User ID are included in each mail message. You are responsible for all electronic mail originating from your User ID. Therefore:

- 2.1 Forgery (or attempted forgery) of electronic mail messages is prohibited.
- 2.2 Attempts to read, delete, copy, or modify the electronic mail of other users are prohibited.
- 2.3 Attempts at sending harassing, obscene, or other threatening e-mail to another user are prohibited.
- 2.4 Attempts at sending unsolicited junk mail, “for-profit” messages, or chain letters are prohibited.

SECTION 3: NETWORK SECURITY

As a user of the network, you may be allowed to access other networks (or the computer systems attached to those networks). Therefore:

- 3.1 Use of systems or networks in attempts to gain unauthorized access to remote systems is prohibited.
- 3.2 Use of systems or networks to connect to other systems, in evasion of the physical limitations of the remote local systems, is prohibited.
- 3.3 Decryption of system or user passwords is prohibited.
- 3.4 The copying of system files is prohibited.
- 3.5 The copying of copyrighted materials, such as third-party software, without the express written permission of the owner or the proper license, is prohibited.
- 3.6 Intentional attempts to “crash” network systems or programs are punishable disciplinary offenses.
- 3.7 Any attempts to secure a higher level of privilege on network systems are punishable disciplinary offenses.
- 3.8 The willful introduction of computer “viruses” or other disruptive/destructive programs into the organization network or into external networks is prohibited.

Signature

Date

User ID

Reference: Wes Morgan (morgan@engr.uky.edu) and Arlene H. Rinaldi (rinaldi@acc.fau.edu). Permission to duplicate or distribute this document is granted with the provision that the document remains intact or if used in pieces, that the original document source be referenced.

Appendix A-4

E-Mail Security Policy

STARCROSS, INC.

E-MAIL SECURITY POLICY

Author(s):	Security Team	Policy Effective Date	July 31, 2004
Approval Authority:	Executive Committee	Policy Last Revised	July 31, 2004
	for Security	Policy Review Date	January 31, 2005

1. Policy Objectives

The electronic mail (e-mail) system is designed to provide an efficient and effective means of communicating throughout all office locations of Starcross, Inc., as well as to external entities with whom Starcross does business. These entities include business partners, vendors, customers, third-party processors, and consultants. Starcross, Inc., provides employees and specified external individuals with e-mail resources to assist and facilitate business communications in the performance of their job-related duties and responsibilities. E-mail is a tremendous productivity tool that also exposes Starcross, Inc., to risks related to the transmission of e-mail messages across local, wide, and public networks. The objective of this policy is to provide you with an understanding of those risks and directives on appropriate use and protection of the system and enterprise information.

2. Electronic Mail Acceptable Use Policy

- a. The e-mail system in its entirety is the property of Starcross, Inc. The system includes e-mail software, PC and server hardware, networks, mailboxes, addresses, user IDs, and passwords. All messages are records of Starcross, Inc.
- b. The e-mail system will be used for company business and as a source of information and efficient communication by employees, management, and privileged users of the system. Incidental personal use is permitted.
- c. Users will protect the use of their e-mail account with a password that is defined according to the password standards and security procedures in the Information Security Policy and the SS&PM for the enterprise.

INFORMATION SECURITY ARCHITECTURE

- d. Electronic mail carried across other networks such as local, regional networks or the Internet are subject to acceptable use policies of those other networks.
- e. Supervisors, system operators, and managers may review the e-mail communications of those using the system to ensure the security of the system, compliance with policy, or determine unauthorized actions on the part of employees or those attempting to access the system.
- f. The company reserves the right to monitor e-mail messages, and to disclose the content of messages to law enforcement officials without prior notice to the user of the system.
- g. Confidential or proprietary information will not be transmitted over the e-mail system. Certified mail or courier will be used for all sensitive information.
- h. Inappropriate use of the system includes but is not limited to:
 - i. Unauthorized access attempts to other e-mail accounts, which includes read, copy, modify, or deletion of messages
 - ii. Transmission of messages from another individual's account without the proper authority or permission
 - iii. Transmission of Starcross confidential or proprietary information to unauthorized individuals or organizations
 - iv. Transmission of obscene, derogatory, harassing, or threatening messages or files to another individual
 - v. Transmission of junk mail, chain letters, personal for-profit business or counterproductive messages that tie up system resources and are not considered in support of Starcross, Inc., objectives
 - vi. E-mail will not be used for wrongful or illegal purposes.
 - vii. E-mail will not be used to download software or files without the use of appropriate virus-checking software procedures.

3. Guidelines for Effective Use of Electronic Mail

- a. The confidentiality of your message cannot be guaranteed. Messages can be misdirected or forwarded to others by the message recipient. Due to contracts or litigation, message files may have to be provided to third parties. Conduct yourself on e-mail as if you were in a public meeting.
- b. E-mail messages create a record. Backup copies are made by the e-mail administrators, and because you have deleted it on your hard drive does not necessarily mean that the backup copy has also been deleted. The recipient may also retain and copy the message. Treat e-mail messages as if they were a permanent record.
- c. Separate opinion from non-opinion and clearly indicate in your message your opinion from that of Starcross, Inc.

- d. Be aware that e-mail messages cannot be retracted once they have been sent. Emotionally charged messages may not be perceived as positive or in the best interest of the enterprise. The ease of use of e-mail makes it difficult to wait until you are ready to respond to an issue in a reasonable manner.
- e. Be selective in sending messages to listservers, interest groups, bulletin boards, etc.
- f. Consider using another method when communicating with customers. Evaluate if the communication needs to be documented and filed in the customer folder to provide consistency and compliance with customer service objectives.
- g. Notify the intended recipient for messages received in error.

4. Violation of Policy

Starcross, Inc., will review alleged violations of this policy on a case-by-case basis. Violations of policy will result in appropriate action, such as written notification to the user of unacceptable actions, loss of electronic mail privileges, loss of computer privilege, and disciplinary actions to include suspension, termination, or referral to appropriate authorities for legal or criminal proceedings.

Your signature indicates that you have read and understand the directives that are outlined in this policy. Use of the e-mail system indicates that you consent to monitoring, access, and disclosure of all messages received and sent by you through the use of the Starcross, Inc., electronic mail system.

Signature

Date

(Printed Name)

Social Security Number

Appendix A-5

Internet Policy

STARCROSS, INC.

INTERNET POLICY

Author(s):	Security Team	Policy Effective Date	July 31, 2004
Approval Authority:	Executive Committee	Policy Last Revised	July 31, 2004
	for Security	Policy Review Date	January 31, 2005

1. Introduction and Background

Business development and objectives include increased productivity, sales, and market targets and have increased the use of the Internet for e-mail, Web pages, electronic commerce, and industry research at Starcross. This increase in Internet use results in both known and unknown risk to the processing environment and makes it necessary for higher security requirements related to its use. Each individual authorized to use this resource must do so appropriately and must take necessary precautions in its use.

2. Objective

This policy establishes a controlled framework for providing access to the Internet and Web. It provides direction and guidance regarding Internet use and covers the exchange of information with other Internet users, both internal and external to the organization. It is established to ensure compliance of Internet use with all organizational policies and laws governing Starcross.

3. Policy Statement

- Use of the Internet for e-mail, Web searches, authorized business transactions, Web development, and research is permitted for business use only by employees of Starcross who have requested and received appropriate authorization. Use of these resources will support the business objectives of Starcross.
- All users granted authorization to use the Internet will receive required training prior to being given a User ID and password.

INFORMATION SECURITY ARCHITECTURE

- Users will acknowledge that they have received training, read and understood the Internet, e-mail, and related policies governing appropriate use by signing the related acknowledgment form.
- Access to the Internet will be through the Intranet Web site and firewall. Establishment of Internet connection through remote access, modems, or individual Internet service provider accounts is prohibited.
- All files downloaded from the Internet will be scanned for viruses at the firewall and on the user's desktop. Users are advised that the frequency of new viruses is high and anti-virus software may not contain definitions to clean the most recent viruses. For this reason, downloading of files from unknown sources is prohibited. The user assumes full responsibilities for any viruses entering Starcross through the downloading of files from the Internet.
- Use of Internet resources for personal business, e-mail, Web-surfing, and the development of personal Web sites is strictly forbidden.
- Chain letters, inappropriate humor, offensive graphics or images, and sexually or racially charged statements are strictly forbidden and will result in termination of employment.
- All users will present a professional image whether through e-mail or Web site presentation.
- Confidential and sensitive information will not be transmitted over a public network, such as the Internet, unless approved authentication and encryption mechanisms have been employed.
- Web-based applications that support marketing will establish mechanisms for authenticating source and destinations of transmissions. No client or potential client information will be transmitted over the Internet without approved authentication and encryption mechanisms in place.
- Use of the Internet for discussion groups for business purposes will represent responses with the following banner: "The views expressed in this message are my own and do not represent that of my employer."
- Users will report any unusual activity or suspected breaches of security to the Information Security Officer.
- All activity must be in compliance with Starcross' Code of Conduct, Information Security Policy, E-mail Policy, Retention Policy, and related standards and procedures in the *Security Standards and Procedures Manual (SS&PM)*.

4. Administration of Policy

- This and all Starcross policies will be fully disseminated throughout the organization.
- All business unit managers will ensure that each staff member is provided this policy, reads and understands his or her rights and obligations as defined.

- Related policies and documents are the Information Security Policy, the Information Security Acknowledgment Form, the E-mail Policy, and the SS&PM.

5. Enforcement of Policy

Starcross, Inc., will review alleged violations of this policy on a case-by-case basis. Violations of policy will result in appropriate action, such as written notification to the user of unacceptable actions, loss of electronic mail and Internet privileges, loss of computer privilege, and disciplinary actions to include suspension, termination, or referral to appropriate authorities for legal or criminal proceedings.

Your signature indicates that you have read and understand the directives that are outlined in this policy. Use of the Internet indicates that you consent to monitoring, access, and disclosure of all messages, files, and transactions received and sent by you through the use of the Starcross, Inc., Internet interface.

Signature

Date

(Printed Name)

Social Security Number

Appendix A-6

Security Lists

This appendix provides Internet resource links to allow you to get started on security topic searches and to sign up for security-related mailing lists.

1. <http://www.cerias.purdue.edu/coast/> — COAST — Computer Operations, Audit, and Security Technology is a multiple-project, multiple-investigator laboratory in computer security research in the Computer Sciences Department at Purdue University. It functions with close ties to researchers and engineers in major companies and government agencies. Their research is focused on real-world needs and limitations, with a special focus on security for legacy computing systems. Professor Gene Spafford is the Director of COAST.
2. <http://www.cerias.purdue.edu/coast/archive/> — The security archives at Purdue are claimed to be the largest single archive on the Internet of papers, tools, standards, reports, mailing lists, and other information related to computer security, law, incident response, and information protection.
3. <http://www.greatcircle.com/> — GreatCircle, Firewalls mailing list. This site uses Majordomo, a program that automates the management of Internet mailing lists. The Firewalls mailing list is the leading forum for discussions of Internet and intranet firewall security systems and related issues.
4. <http://www.cs.uwm.edu/faculty/levine/cpd.homepage.html> — Computer Privacy Digest. The Computer Privacy Digest (CPD) is a forum for discussion of the effect of technology on privacy. The digest is linked into the USENET newsgroup comp.society.privacy. This forum is designed to discuss the effect that technology has on privacy. The forum is sent out in a digest format. Submissions to the digest should be sent to comp-privacy@uwm.edu.
5. <http://www.xforce.iss.net> — This link takes you to the Internet Security Systems, Inc., Web page and Xforce, which provides security advisories, publications outlining current security trends and issues, and links to security mailing lists. The link <http://www.xforce.iss.net/xforce/maillists/> contains links to the following mail lists and publications: SecTech, SecNews, NT Security, NSA, Alert, NSA Forum, ISS forum, X-Press, Intrusion Detection Systems.
6. <http://www.SecurityFocus.com> — This Web page provides links for research on many security topics and recent publications. The Web

page contains the latest articles on security news, vulnerabilities, tools, a library archive, forums, and an updated event calendar for security presentations and conferences.

7. http://dir.yahoo.com/Computers_and_Internet/Security_and_Encryption/ — The categories listed under the Yahoo search engine for computer security are:

Anonymous Mailers	Hacking	Risks
Books@	Information Warfare@	RSA
Challenges	Institutes	S/KEY
Computer Immune Systems	Java@	Software
Conferences	Kerberos	Software Piracy@
Cryptography	Magazines	Steganography
Developers, Products and Services@	Mailing Lists	Unix@
Digital Money@	MD5	Viruses and Worms
Digital Signatures	Organizations	Web Directories
Encrypted Email Providers@	PGP—Pretty Good Privacy	WWW Security@
Encryption Policy	Privacy@	X Windows@
Firewalls	Rijndael	FAQs

8. <http://www.counterpane.com/crypto-gram.html> — The Counterpane Internet Security, Inc., Web site offers the Crypto-Gram Newsletter at this link.
9. <https://www.gartner.com/> — The Gartner Group Web site provides research on a wide variety of industry topics relating to technology. A complimentary log-in ID is available but does not provide access to publications available only for purchase. Many organizations have Gartner Group subscriptions that are tailored to the industry and technology of the organization and are charged accordingly.

Appendix A-7

Security Standards and Procedures Manual Table of Contents

Security Standards and Procedures Manual Table of Contents

- 1.0 Account Management
 - 1.1 Log-in Accounts
 - 1.1.1 System Administrator Log-in Accounts
 - 1.1.2 User Accounts
 - 1.1.3 Log-in Account Suspension, Reactivation, and Removal
 - 1.1.4 Concurrent Connections
 - 1.1.5 User Menus
 - 1.1.6 Groups
 - 1.1.7 Warning Banners
 - 1.1.8 Access to System Prompt
 - 1.1.9 Global Volume Access
 - 1.1.10 Individual Accountability
 - 1.1.11 Shared Systems
 - 1.1.12 Separation of Duties
 - 1.1.13 Vendor/Contractor Access
 - 1.1.13.1 Confidentiality Agreements
 - 1.1.13.2 Awareness & Training
 - 1.1.14 Customer Access
 - 1.1.14.1 Transaction Processing
 - 1.1.14.2 Inquiry Processing
 - 1.1.14.3 Remittance Confirmation
 - 1.1.15 Naming Standards
 - 1.1.16 Suspension of Accounts
 - 1.1.17 Deletion of Accounts
 - 1.2 Passwords
 - 1.2.1 Screen Saver Passwords

INFORMATION SECURITY ARCHITECTURE

- 1.2.2 Sharing of Passwords
- 1.2.3 Password Minimum Length
- 1.2.4 Password Expiration
- 1.2.5 Password History File
- 1.2.6 Password Changes
- 1.2.7 Password Suspension and Reset
- 1.3 Personnel Orientation, Transfer, and Termination
 - 1.3.1 New User Orientation
 - 1.3.2 Security Awareness Program
 - 1.3.3 Revoking Access of Terminated or Transferred Employees
 - 1.3.4 Revalidation of Confidentiality Agreement
- 2.0 Resource Management
 - 2.1 Resource Ownership
 - 2.1.1 Owner
 - 2.1.2 Custodian
 - 2.1.3 User
 - 2.1.4 Security Administrator
 - 2.1.5 Security Liaison
 - 2.1.6 Classification of Resources
 - 2.2 Confidentiality
 - 2.2.1 Privacy Principles
 - 2.2.2 Public
 - 2.2.3 Sensitive
 - 2.2.4 Confidentiality
 - 2.2.5 Copying and Printing
 - 2.2.6 Transmission and Shipping
 - 2.3 Integrity
 - 2.3.1 Data Entry
 - 2.3.2 File Integrity
 - 2.3.3 Transmission Integrity
 - 2.3.4 File Modification
 - 2.3.5 Reconciliation
 - 2.4 Availability
 - 2.4.1 Backups
 - 2.4.1.1 System Archival & Storage
 - 2.4.1.2 PC Archival & Storage
 - 2.4.2 Continuity Planning
 - 2.4.2.1 Business Impact Analysis
 - 2.4.2.2 Risk Assessment
 - 2.4.2.3 Recovery Alternatives
 - 2.4.2.4 Continuity Plan Development
 - 2.4.2.5 Testing
 - 2.4.3 Disaster Recovery Planning
 - 2.4.3.1 Testing
 - 2.5 Authentication

Security Standards and Procedures Manual Table of Contents

- 2.5.1 Authentication Methodology
- 2.5.2 Strong Authentication
- 2.5.3 Scripts/Automatic Logins
- 2.5.4 User Validation
- 2.6 Encryption
 - 2.6.1 Algorithms
 - 2.6.2 Strength
 - 2.6.3 Key Management
 - 2.6.4 Digital Signatures
 - 2.6.5 Digital Certificates
- 2.7 Information Storage
 - 2.7.1 Hard Copy
 - 2.7.2 Electronic
 - 2.7.3 E-mail
 - 2.7.4 Voicemail
 - 2.7.5 Retention Plan
- 2.8 Information Destruction
 - 2.8.1 Hard Copy
 - 2.8.2 Electronic
 - 2.8.3 E-mail
 - 2.8.4 Voicemail
- 2.9 Laptop Security
 - 2.9.1 Personally Owned Computers
 - 2.9.2 Information Storage
 - 2.9.3 Physical Controls
 - 2.9.4 File Backup
 - 2.9.5 Anti-Virus Controls
 - 2.9.6 Travel Considerations
 - 2.9.7 Laptop Theft
- 2.10 System Maintenance
 - 2.10.1 Application Maintenance
 - 2.10.2 Operating System Maintenance
 - 2.10.3 PC Repair, Transfer, and Disposal
 - 2.10.4 Booting of PCs from Diskettes
- 2.11 Change Control
 - 2.11.1 Change Management Process and Approval
 - 2.11.2 Separation of Production and Test Environments
 - 2.11.3 Access to Production Information for Testing
- 3.0 Network/Communications Security
 - 3.1 Dial-Up Access Controls
 - 3.1.1 Dial-Up Authentication
 - 3.1.1.1 Employee Connections
 - 3.1.1.2 Customer Connections
 - 3.1.1.2.1 Legal/Contractual Agreements
 - 3.1.1.3 Vendor Connections
 - 3.1.1.3.1 Legal/Contractual Agreements
 - 3.2 Dial-Out Connections

INFORMATION SECURITY ARCHITECTURE

- 3.3 Internet Connections
 - 3.3.1 Demilitarized Zone (DMZ)
 - 3.3.2 Containment/Isolation
 - 3.3.3 Firewalls
 - 3.3.4 Routers
 - 3.3.5 Inbound/Outbound Access Restrictions
 - 3.3.6 Content Control
- 3.4 TCP/IP Connections
- 3.5 Non-Dedicated/Shared WAN
- 3.6 Electronic Mail
 - 3.6.1 Shared Accounts
 - 3.6.2 Transmission of Sensitive Information
 - 3.6.3 Personal Usage
 - 3.6.4 Forwarding Messages
 - 3.6.5 Accessing E-mail from Home
 - 3.6.6 Chain Mail
 - 3.6.7 Retention
- 3.7 Private Branch Exchanges (PBX)
 - 3.7.1 Voicemail
- 3.8 Cellular Telephones
- 4.0 Physical Security
 - 4.1 Environmental Controls
 - 4.1.1 Fire
 - 4.1.2 Water
 - 4.1.3 General
 - 4.2 Physical Access Controls
 - 4.2.1 Building Access
 - 4.2.2 Data Center Access
 - 4.2.3 Identification
 - 4.2.4 Logging
 - 4.2.5 Visitor Access
 - 4.2.6 Photography
- 5.0 Security Monitoring and Compliance
 - 5.1 Data Security Monitoring Scope and Responsibilities
 - 5.1.1 Event Logs
 - 5.1.2 Access to Event Logs
 - 5.1.3 Logging of Privileged Accounts
 - 5.2 Anti-Virus Detection
 - 5.2.1 Definition Maintenance
 - 5.2.2 Logging
 - 5.2.3 Reporting
 - 5.3 Incident Response
 - 5.3.1 Logging
 - 5.3.2 Reporting
 - 5.3.3 Escalation
 - 5.3.4 Emergency Response
 - 5.3.5 Investigation

Security Standards and Procedures Manual Table of Contents

- 5.4 Alerts, Advisories, and Notices
 - 5.4.1 Sources
 - 5.4.2 Dissemination
- 5.5 Vulnerability Testing
- 5.6 Security Certification
- 6.0 Security Awareness & Training
 - 6.1 Program Development
 - 6.2 New Hire Orientation
 - 6.3 Confidentiality Agreement
 - 6.4 Code of Ethics
 - 6.5 Annual Training of Employees
 - 6.6 Contractor/Vendor Training
 - 6.7 Security Awareness Communications
- 7.0 Legal & Regulatory Compliance
 - 7.1 Acquisition of Software
 - 7.2 Software License Requirements
 - 7.3 Use of Freeware
 - 7.4 Applicable Federal & State Regulations
 - 7.5 Information Misuse
 - 7.6 Non-Compliance to Policies and Standards

Appendix A-8

Anti-Virus Update Procedure

STARCROSS, INC.

ANTI-VIRUS UPDATE PROCEDURES

Author(s):	Anti-Virus Program Manager	Procedure Effective Date	July 31, 2004
Review Authority:	Security Team	Procedure Last Revised	July 31, 2004
		Procedure Review Date	Jan 31, 2005

PROGRAM OVERVIEW

The Starcross Anti-Virus Program is designed to protect processing resources from the threat of malicious code. This is performed through a three-tiered architecture:

1. Client workstation/server — using Symantec's Norton Anti-Virus
2. Lotus mail servers — using Trend Micro's ScanMail
3. Firewalls — using Trend Micro's InterScan Viruswall

COMPONENTS OF THE PROGRAM

The current process to download and disseminate virus updates is described in this section.

A. Client Workstation/Server

Win 9x, Windows NT, DOS, and Windows XP run the Norton Anti-Virus version certified for each client.

1. The Information Security Operation's Group anti-virus administrator downloads Symantec site virus updates biweekly from the Symantec Web site at www.symantec.com. Specific instructions for downloading virus definitions are provided in internal document Anti-Virus Download.doc on the Security Intranet Web site at www.starcross.com/security/antivirus/antiv13.html. This document provides download and deployment instructions. Updates will be placed on servers `snetw1`, `scent1`, for initial testing.

INFORMATION SECURITY ARCHITECTURE

2. Tested updates are forwarded to the Netware Administrator in Server Support to initiate production testing on several Netware servers running different services.
3. The Netware Administrator then distributes updates to all Netware Administrators at all Starcross remote operating locations with an explanation of how to configure Netware servers to distribute updates to workstations. This document is located on the Security Intranet Web site at www.starcross.com/security/antivirus/antiv14.html.
4. Netware Administrators will receive instruction on log-in script testing to ensure the update has been loaded properly. Norton's update utility is run to verify the correct signature version.
5. Live updates are performed biweekly from scnetw3 server to ensure that clients have the most recent version. This update is a failover process if administrators fail to copy and distribute the most recent version of the update. Load balancing is performed by staggering update times for each client.

B. Lotus Mail Servers

ScanMail by Trend Micro is used to scan all Lotus Notes servers.

1. Lotus Notes Server scln004 automatically attaches to the Trend Micro Web site on Sunday evening and downloads the latest virus definitions. A script has been written to automatically push these definitions to all the other Notes servers.
2. All outbound and inbound mail attachments are scanned for viruses. Unsuccessful attempts to clean infected files are automatically placed in a quarantine directory. The Lotus Notes administrator reviews the quarantine directory on Monday mornings to investigate potential virus issues. These issues are registered as necessary in the Problem Status Review meetings held every Tuesday afternoon. Manual intervention and review of all quarantined files is necessary to resolve potential virus issues. Cleaned files are forwarded to the appropriate destination by the Lotus Notes Administrator.

C. Virus Wall

Trend Micro software is used to scan all files inbound and outbound through all firewalls.

1. An automated download of the update from the Trend Micro Web site is performed weekly on Saturday evenings to the schpux01 server. The update is then distributed automatically to all other firewall platforms.
2. Emergency update procedures can be performed using the fwvirus program located at www.starcross.com/security/antivirus/fwvirus.exe.

TESTING

Anti-virus version upgrades are tested on scnetw1 and scnt1 servers. Testing is also performed to verify that live updates via automated distribution from server to clients are completed.

Live update scan schedules are validated monthly to ensure that all clients are updated. Update schedules are validated against the server database to ensure that new server implementations are added to the live update schedule.

Verification is performed to ensure that the latest updates to virus definitions and the software engine are stable in new versions of anti-virus software.

Appendix B-1

Security Assessment Workplan

INFORMATION SECURITY ASSESSMENT WORKPLAN

Organization: _____

Business Unit: _____

Review Conducted on: _____

Review Conducted by: _____

This assessment workplan is designed to provide an understanding of the security posture of the organization. The three sections of this workplan are designed to provide a high-level overview of the security posture of the organization. Section I concentrates on obtaining an understanding of the operating environment, the management of specific programs developed as a part of the ISA, and the allocation of security responsibilities. Section II provides an overview of operational security programs. Section III focuses on the security of computer operations. Separate workplans are directed at the security of specific components of the operating environment: networks, applications, databases, and operating systems.

SECTION I: OPERATING ENVIRONMENT, SECURITY ADMINISTRATION, AND MANAGEMENT

1.0 Operating Environment

1-1 Mainframe environment (include number of each)

- MVS with RACF _____
- MVS with ACF2 _____
- MVS with Top Secret _____
- IBM VM MVS _____
- ICL VME _____

INFORMATION SECURITY ARCHITECTURE

1-2 Midrange Computers (include number of each)

- AS/400 _____
- DEC VMS _____
- HP/3000 MPE _____
- UNIX _____
- Ultrix _____
- Sun OS _____
- Solaris _____
- HP _____
- IBM AIX _____
- SCO UNIX _____
- Stratus _____
- Tandem _____

1-3 PC Network Operating Systems

- UNIX _____
- Novell Netware _____
- Windows NT _____
- OS/2 _____
- Banyan Vines _____

1-4 Desktop Platforms

- DOS _____
- Windows 3.x _____
- Windows 95 _____
- Windows 98 _____
- Windows 2000 _____
- Windows NT Workstation _____
- OS/2 _____

1-5 Describe control mechanisms for remote access (check all that apply).

- Modem only (password and ID)
- Tokens (dual authentication)
- Remote Access Server (RAS)
- Single-use passwords

1-6 List all wide area network connections and extranet connectivity (include number of lines).

- Frame Relay _____
- ISDN dial _____
- VPN _____
- Value-Added Network (VAN)
- Microwave
- Other _____
- _____
- _____

- 1-7 List e-mail software and number of servers. _____
- 1-8 List Internet service providers (ISP) and all authorized methods of connecting to the Internet.

- 1-9 List Internet browser software authorized for use.

- 1-10 List projected technology and application implementations.

Provide a detailed explanation for each of the following questions.

2.0 Security Organization

- 2-1 How many full-time equivalent (FTE) positions exist for the management of the security function?
- 2-2 Describe the positions and the major responsibilities of each FTE.
- 2-3 Are third-party or consulting services employed for any portion of the security function? Describe who, when, how often, and for what purpose.
- 2-4 Have job descriptions, duties, and responsibilities for the various security personnel, such as the Information Security Officer, Access Control Administrator, Security Project Manager, been defined and documented?
- 2-5 Who does the security function fall under, the Chief Information Officer (CIO), the Chief Financial Officer (CFO), or directly to the Chief Executive Officer (CEO)?
- 2-6 Is the security organization's operation and planning reviewed by a Steering Committee, Executive Counsel, or Board of Directors?

INFORMATION SECURITY ARCHITECTURE

- 2-7 Describe how the security organization maintains its independence from other business units in enforcing policies and standards and assessing compliance.
- 2-8 Describe the positions or personnel responsible for the following programs: Security Awareness and Training Program, access request and implementation, emergency and incident response procedure development and execution.
- 2-9 What role do security personnel play in system development and software acquisition? How are security requirements communicated in this process?

3.0 Information Security Plan

- 3-1 Has an Information Security Plan been developed and documented? (Provide a copy)
- 3-2 Who is responsible for development, review, implementation, and approval of the Information Security Plan?
- 3-3 Does the plan support the goals and objectives of the Strategic Information Technology Plan?
- 3-4 How do business unit managers, resource and application owners provide input to the Information Security Plan?
- 3-5 Are performance measures and benchmarks linked to the goals and objectives of the Information Security Plan?
- 3-6 Are estimated and actual losses related to security incidences and lack of system availability calculated, quantified, and reported?
- 3-7 Are responsibilities and target completion dates defined for each project, initiative, or strategy identified in the Security Plan?
- 3-8 Is there an Information Security Architecture or Security Framework in place?
- 3-9 How does management ensure that security controls and procedures are enforced, updated, and tested?
- 3-10 How is effectiveness of the security program measured? Is this quantification formally reported to an executive officer, committee, or board?

- 3-11 What means of communication exist for business unit managers to report the status of security implementations as a part of the management review process?
- 3-12 Is there a formal security awareness program?
- 3-13 Does security awareness begin at new-hire orientation? What programs have been integrated with Human Resource responsibilities to appropriately address security policy, confidentiality, and the protection of organizational resources?

4.0 Security Policies, Standards, and Procedures

- 4-1 Is there a high-level policy that describes the organization's goals and objectives related to security?
- 4-2 How are policies developed, reviewed, and approved and who is responsible for each step of this process?
- 4-3 How are security standards developed?
- 4-4 Does the policy cover:
 - The employee's responsibility to protect information assets?
 - Ownership of resources?
 - Inappropriate use of resources?
 - Security management and administration?
 - Classification of information by risk and monetary loss?
 - Information access control?
 - User identification and authentication?
 - Security monitoring?
 - Software licensing?
 - Storage, retention, and destruction of information?
- 4-5 How do business unit managers and resource owners provide input to the policy, standards, and procedures development process?
- 4-6 How do each of the business unit's policies, standards, and procedures support the corporate policies and standards?
- 4-7 Does the security policy encompass all information obtained, created, and maintained by the organization to include verbal, electronic, hard-copy, and voice messaging?
- 4-8 How do each of the business unit's own policies, standards, and procedures support the corporate policies and standards?

INFORMATION SECURITY ARCHITECTURE

- 4-9 How are changes to the policies, standards, and procedures initiated, reviewed, and communicated throughout the organization?
- 4-10 Does the security policy include written rules, penalties, and associated disciplinary action against individuals who compromise important security measures and safety practices? Have those penalties been reviewed by legal and deemed enforceable?
- 4-11 Is there a formal process that ensures employees have read the information security policy and understand their responsibilities to uphold its contents?
- 4-12 Are confidentiality agreements or nondisclosure agreements signed at new-hire orientation?
- 4-13 How are these agreements updated for current employees?
- 4-14 How is compliance to policies and standards enforced?

5.0 Risk Assessment

- 5-1 What method is there to classify data based upon its sensitivity? What method exists to ensure that the protection of information is commensurate with its level of classification?
- 5-2 What methods are used by employees to report to management any information pertaining to fraud, corruption, conflict of interest, theft, vandalism, or computer modifications committed by a fellow employee or persons dealing with the organization? Does the security policy detail these methods?
- 5-3 Who has been assigned the responsibility within the information security program to conduct periodic risk assessments?
- 5-4 How often are risk assessments conducted?
- 5-5 Have key risks been identified and documented?
- 5-6 Has a risk mitigation plan been developed that addresses those key risks?
- 5-7 Are Business Impact Analyses conducted to determine losses related to business interruption and typical or realistic threat scenarios?

- 5-8 Have Business Continuity Plans and Disaster Recovery Plans (BCP/DRP) been developed based upon the recovery of critical business functions?
- 5-9 Are BCP and DRP plans tested annually? Are business units involved in testing BCP/DRP plans?
- 5-10 What are the business functions critical to ongoing operations?
- 5-11 How often are BCP/DRPs reviewed and revised?
- 5-12 How are information and system resource owners identified and documented? What responsibilities are assigned to these resource owners?
- 5-13 How are security incidences and violations monitored, investigated, and improvements made related to the incident?

SECTION II: OPERATIONAL SECURITY PROGRAMS

6.0 Security Monitoring

- 6-1 Do security monitoring procedures exist to identify and investigate suspected access violations and attempted system intrusions? This includes audit trails of security-related events.
- 6-2 Are responsibilities for security monitoring defined and documented?
- 6-3 Are remote access logs reviewed to identify failed log-in attempts?
- 6-4 Are system access logs reviewed for access to systems during non-working hours, weekends, and holidays?
- 6-5 Is access to application system utilities and privileged user activities reviewed?
- 6-6 How often is traffic on external gateways and dial-in connections reviewed?
- 6-7 Is a review conducted of access to sensitive files or data?
- 6-8 Is there a procedure for reporting potential or suspected security violations?
- 6-9 How are these procedures communicated throughout the organization so that all users know how and can report suspected activity?

INFORMATION SECURITY ARCHITECTURE

6-10 Do procedures include notification, escalation, investigation, reporting, analysis, and remediation?

7.0 Computer Virus Controls

7-1 Is a comprehensive anti-virus program in place, documented, and measured for effectiveness?

7-2 What type of anti-virus software is used on:

Workstations?

Mail servers?

Firewalls?

7-3 How often are current virus definitions downloaded from the appropriate sources?

7-4 Where are virus definitions obtained? Are procedures documented to download definitions from the source and to test, distribute, load definitions to the appropriate platforms?

7-5 How is compliance with anti-virus procedures tested to ensure full support of the program?

7-6 Does a procedures exist for users to report potential or suspected viruses?

7-7 Do security personnel research virus alerts to ensure that all organization systems are protected against known viruses?

7-8 How is virus information communicated to users to alert them of the most recent strains of damaging viruses?

8.0 Microcomputer Security

8-1 Do security guidelines or PC usage policies exist and are users trained on appropriate use of systems to include physical and logical access controls?

8-2 Are anti-theft devices such as cables and locks utilized?

8-3 Are offices, work rooms, and buildings where PCs are located locked at night?

8-4 Are computer disks and tapes appropriately labeled and stored in locked facilities?

- 8-5 Is software loaded and enabled to prevent unauthorized access to PCs and laptops?
- 8-6 Is software available to encrypt hard drives or sensitive data and programs to prevent unauthorized access?
- 8-7 Is software designed to timeout and lock inactive workstations?
- 8-8 Are PCs and laptops inventoried for registered software to ensure that all programs and software are approved, licensed, and appropriately registered?
- 8-9 Are approved software lists defined and distributed to users?
- 8-10 What procedures exist to monitor licenses registered versus licenses used?
- 8-11 Is an asset inventory performed and does it include serial numbers to assist in the recovery of assets if lost or stolen?
- 8-12 Do all laptops and PCs have up-to-date virus detection software loaded?
- 8-13 Are virus scans automated?
- 8-14 Do PC usage policies define the use of anti-virus software and warn against disabling or reconfiguring system utilities or security tools?
- 8-15 Are PC applications defined in-house? Does PC software development comply with the organization's software development methodologies?
- 8-16 Have backup and contingency plans been developed for PCs and laptops?

9.0 Compliance with Legal and Regulatory Requirements

- 9-1 Does the design, operation, and use of information systems comply with industry regulations?
- 9-2 What department or job function has been assigned the responsibility of researching, understanding, and communicating legal and regulatory requirements for the industry?
- 9-3 How is compliance to industry regulations measured?
- 9-4 Are standards defined on the retention, storage, and handling of regulated information?

INFORMATION SECURITY ARCHITECTURE

- 9-5 Does a classification methodology exist to categorize information according to value or sensitivity? Does this methodology correspond with the classifications according to regulations?

SECTION III: COMPUTER OPERATIONS SECURITY

Computer operations includes physical and environmental security of processing hardware and software, the daily execution of programs, the backup of data and programs, and problem management of any issues that arise from errors or improper execution of programs.

10.0 Physical and Environmental Security

- 10-1 Are all data processing facilities protected against unauthorized physical access?
- 10-2 Is physical access to computing facilities limited to essential personnel required access to perform their job functions?
- 10-3 Is the computing facility shared with other businesses, business units, or departments?
- 10-4 What type of businesses, business units, or departments share the facilities?
- 10-5 What controls guard against unauthorized access to computing facilities?
- Security guards
 - Cypher locks
 - Keypad locks
 - Fencing
 - Motion detectors
 - Sensors
 - Alarms
 - Badges
 - Personnel access lists
 - Sign-in logs
- 10-6 Is the computing facility located away from environmental hazards (i.e., fuel sites, airports, chemical plants, waste dumps, dams, rivers)?
- 10-7 What environmental controls are in place to minimize damage due to fire, flood, or other natural disasters?

- Backup power (Uninterruptible Power Systems - UPS)
- Air conditioning
- Fire suppression devices (fire extinguishers, halon, other)
- Fire detection devices (sensors)
- Heat detection devices
- Business Continuity Plans (BCP)
- Alternative processing facilities

11.0 Computer Systems Management

- 11-1 Are responsibilities for the management and operation of all computer systems clearly defined?
- 11-2 Do computer operations procedures exist for daily operations so that backup personnel can understand and follow written guidance on daily processes?
- 11-3 Is a log maintained for the execution, completion, and errors that occur during each shift?
- 11-4 Are shift change procedures clearly defined to include joint log reviews and a synopsis of all issues incurred during prior shift operations?
- 11-5 Are logs reviewed daily by supervisors?
- 11-6 Are computer operations personnel restricted from read, write, and delete access of computer programs?
- 11-7 Are computer operations personnel restricted from source code access and limited to only executable programs?
- 11-8 Are computer operations personnel restricted from moving compiled programs from test to production environments?
- 11-9 Are separate development, test and production systems, and processing environments maintained?
- 11-10 Are change control procedures documented and do they include a process for reviewing the status of changes on a weekly basis?
- 11-11 How is change management communicated to users, management, and departments affected by implementation of the change?

INFORMATION SECURITY ARCHITECTURE

12.0 Backup and Recovery Planning

- 12-1 At what interval are full system backups performed?
- 12-2 At what interval are incremental backups performed for system configurations, programs, and data?
- 12-3 What is the rotation schedule for backup tapes for:
 - Full system?
 - Incremental data?
- 12-4 Are backup tapes maintained off-site?
- 12-5 Where are backup tapes stored?
- 12-6 Is a third-party vendor contracted for backup storage and rotation?
- 12-7 If a third-party vendor is used, where are tapes dropped off and picked up, and what control exists to ensure that the tapes are not exposed to unauthorized access?
- 12-8 Describe the management system for disk and tapes.
- 12-9 How are backups labeled and logged?
- 12-10 How often are backup restoration procedures performed?
- 12-11 Does testing include full system testing?
- 12-12 Does a Disaster Recovery Plan exist?
- 12-13 Are third-party vendors used for DRP?
- 12-14 Are non-disclosure agreements signed by vendors?
- 12-15 Is a current SAS-70 for all third-party processing facilities maintained and have they been reviewed?
- 12-16 When was the DRP last reviewed and tested?
- 12-17 Has a full system test of DRP been performed that included restoration to an alternate facility?
- 12-18 Does the DRP include different scenarios for recovery planning?

- 12-19 What off-site facilities exist for Disaster Recovery?
- 12-20 Does a Business Continuity Plan (BCP) exist that prioritizes the recovery of critical systems and information?
- 12-21 Has a Business Impact Analysis been performed to support the BCP and DRP? When was the last Business Impact Analysis performed? Has the computing environment changed significantly since the BIA? (i.e., have mainframe or minicomputer systems migrated to client server?)

13.0 Problem Management

- 13-1 Is a problem management process in place to document, report, analyze, and resolve problems?
- 13-2 Do procedures include notification, escalation, investigation, reporting, analysis, and remediation and are these procedures documented?

Appendix B-2

Application Security Assessment

APPLICATION SECURITY ASSESSMENT

<i>Business Unit:</i> _____
<i>Application:</i> _____
<i>Platform/Operating System:</i> _____
<i>Review Conducted on:</i> _____
<i>Review Conducted by:</i> _____

1.0 Operating Environment: This section is intended to gather additional detail related to the operating environment and the application interfaces.

- 1-1 How many users have access to this application?
- 1-2 What type of network connects data input devices to the application?
- 1-3 What type of data input devices are used?
- 1-4 What type of access control software is used?

- RACF _____
- ACF2 _____
- Top Secret _____
- CICS _____
- Application menu driven _____

INFORMATION SECURITY ARCHITECTURE

1-5 Is remote access used to access the application? If yes, what type of access control mechanisms are used? (check all that apply)

- Modem only (password and ID)
- Remote Access Server (RAS)
- Tokens (dual authentication)
- Single-use passwords

1-6 List all wide area network connections and extranet connectivity that application data traverses.

- Frame Relay _____
- ISDN dial _____
- VPN _____
- Value-Added Network (VAN)
- Microwave _____
- Internet _____
- Other _____
- _____
- _____

1-7 List other applications that are integrated with this application.

1-8 List projected application modifications or technology upgrades related to this application.

2.0 Authorization: Authorization is the process of granting access to specific application data or functions based upon job function and requirements. Authorization needs to be established for each new user of the system. Authorization is also the process of validating established access rights each time a user attempts to access the application.

2-1 Are data, application, and component owners documented and identified?

2-2 Is access to the application data granted upon approval of the data owner?

2-3 Is access granted based on job function?

2-4 Is a formal procedure in place for requesting access, registering users, and modifying access as required? Describe this procedure and any forms used for the registration process.

- 2-5 Is there a formal procedure in place to notify application administrators and data owners to revoke access when an employee leaves the organization?
- 2-6 Are reviews conducted on a quarterly basis to validate that user access is appropriate? Describe the mechanism in place that ensures this review takes place.
- 2-7 Does this periodic review check for inactive accounts and employees who have terminated employment or changed job responsibilities?
- 2-8 Is access restricted by application menus, specific functions, or accounts?
- 2-9 Can access be granted at different levels or modules within the application based on job requirements and functionality to enforce separation of duties?
- 2-10 Is access to source libraries restricted and appropriate?
- 2-11 Does the capability to audit access to source libraries exist and is access being audited?
- 2-12 Are templates used to define access based on job function?
- 2-13 Is user access restricted to application menus so that the user cannot obtain command line access?
- 2-14 Is there a facility for users to lock their screen if leaving it active and unattended?
- 2-15 Does the system automatically timeout if the terminal is inactive for a set standard period of time?
- 3.0 Authentication: Authentication is the assurance that the user who is requesting access is really who the user claims to be. Appropriate authentication is necessary for effective access control.**
- 3-1 Are unique user IDs and passwords assigned for each user of the system?
- 3-2 Is there a procedure or application routine that checks to ensure that user IDs and passwords are not inappropriate, easily guessable, and are within established ID and password guidelines?

INFORMATION SECURITY ARCHITECTURE

- 3-3 Do password controls include automatic restrictions on the type of passwords that can be used (for example, length, type of characters, history files, cycle times, lockout for failed log-in attempts)?
- 3-4 Are users forced to change their passwords on a monthly basis?
- 3-5 Are privileged users required to change their passwords more frequently?
- 3-6 Upon initial log-in, are users forced to change their password immediately?
- 3-7 Are other forms of authentication used? (Check all that apply)
- Single-use passwords _____
 - Biometrics _____
 - Smart cards _____
 - Other _____
- 3-8 Are passwords encrypted across the network, in stored password files, and on backup files?
- 3-9 Is third-party or vendor access controlled by logging all access requirements, resetting passwords, and maintaining audit trails for all maintenance or access?
- 4.0 Integrity: Integrity controls ensure that applications programs and data are accurate and complete.**
- 4-1 Does data input validation exist to ensure that the length of data and the character parameters match the expected values?
- 4-2 Do control programs exist to detect out-of-range values, missing and incomplete data, invalid characters, upper and lower data volume limits, and two-character date ranges?
- 4-3 Is a periodic review conducted to validate the integrity of key fields and data files?
- 4-4 Do session or batch controls exist to reconcile file balances after transaction updates?
- 4-5 Do balance controls exist to validate opening balances with previously closed balances, including run-to-run totals, file update totals, program-to-program totals, and hash totals on records and files?

- 4-6 Do separate test and production environments exist and is access to those environments consistent with segregation of duty restrictions?
- 4-7 Does a program management tool exist to control access and management of program source code?
- 4-8 Define the controls that exist to protect from updating the wrong module of source code.
- 4-9 Define what controls exist to prevent the use of outdated versions of programs.

5.0 Application Development and Implementation

- 5-1 Does a Systems Development Life Cycle (SDLC) methodology exist?
- 5-2 Are there standard procedures for users to request application acquisition, development, or maintenance?
- 5-3 Determine if management authorizes the initiation of application acquisition, development, and maintenance.
- 5-4 How are change requests initiated?
- 5-5 Describe the process from change request initiation to moving tested and approved changes into production.
- 5-6 Define what controls exist to track and report the status of program changes.
- 5-7 Are audit trails of changes made to production versions of programs maintained and reviewed?
- 5-8 Determine if there is change request documentation that records the reason for the amendment, date of amendment, and appropriate approvals.
- 5-9 Is acceptance criteria for test plans documented, approved, and reviewed?
- 5-10 Are there formal sign-off and acceptance procedures?
- 5-11 Are there cutover procedures to move applications from the test to the production environment?

INFORMATION SECURITY ARCHITECTURE

- 5-12 Is segregation of duties maintained between programming and the execution of programs?
- 5-13 Are copies of production code, prior to making the changes, maintained?
- 5-14 Is system and user documentation updated to reflect all program and operations changes?
- 5-15 Are emergency maintenance and temporary fixes to application and system software covered by the same procedures applied to normal maintenance?

6.0 Computer Operations (Specific to an Application)

- 6-1 What application system utilities are enabled?
- 6-2 Are the utilities accessible from the application? Obtain a listing of individuals with approved access to system utilities.
- 6-3 Describe how the utilities are accessed and how access is controlled.
- 6-4 Are procedures for the operation of all computer systems documented?
- 6-5 Is a log maintained of all work performed by computer operators? Is the log reviewed regularly by supervisors to ensure the work is being performed consistently and according to standard?
- 6-6 Define the physical security surrounding the server or mainframe housing the application.

7.0 Database

- 7-1 What type of database is used to store application data?
- 7-2 What applications share access to this database?
- 7-3 What access controls are used to assign access to database information: discretionary access controls, mandatory access controls, or both?
- 7-4 Is access to database information reviewed on a periodic basis?
- 7-5 Do individuals with access to database information and files have command line access?

- 7-6 Obtain a report of all world-writable files. Define who are the individuals that have access to these files. Is the number of individuals with access to these files reasonable? What are the job functions of each of these individuals? Compare the job function with world-writable files accessed and determine if permissions are necessary for each job function.

Appendix B-3

Network Security

Assessment

Workplan

NETWORK SECURITY ASSESSMENT WORKPLAN

<i>Business Unit:</i> _____
<i>Review Conducted on:</i> _____
<i>Review Conducted by:</i> _____

1.0 Network Operating Environment: This section is intended to gather additional detail related to the networking environment.

1-1 List all wide area network connections and extranet connectivity (include number of lines)

- | | |
|--|--|
| <input type="checkbox"/> Frame Relay _____ | <input type="checkbox"/> ISDN dial _____ |
| <input type="checkbox"/> VPN _____ | <input type="checkbox"/> Value-Added Network (VAN) _____ |
| <input type="checkbox"/> Microwave _____ | _____ |
| <input type="checkbox"/> Other _____ | _____ |
| _____ | _____ |
| _____ | _____ |

1-2 List all local area network (LAN) operating systems and the versions used.

- | |
|---|
| <input type="checkbox"/> Novell Netware _____ |
| <input type="checkbox"/> Windows NT _____ |
| <input type="checkbox"/> Banyan Vines _____ |
| <input type="checkbox"/> Other _____ |
| <input type="checkbox"/> _____ |
| <input type="checkbox"/> _____ |

INFORMATION SECURITY ARCHITECTURE

1-3 Are the networks:Wiring:

- Token Ring? _____
- Ethernet? _____

1-4 How many physical sites are connected through the network?

1-5 List e-mail software and number of servers. _____

1-6 Is e-mail limited to specific users within the organization or is it used organizationwide?

1-7 How many e-mail accounts are there?

1-8 List Internet service providers (ISPs) and all authorized methods of connecting to the Internet.

1-9 List Internet browser software authorized for use.

1-10 Is the network center restricted to authorized personnel?

- Restricted access to the network control center
- Physical security mechanisms are implemented to restrict access
- Communications controllers are located in a secure area
- Cables and wiring are unexposed and wiring closets are locked at all times
- All visitors are required to sign in
- All visitors are required to wear visitor badges
- Access restrictions are documented

1-11 Is the network control center protected against environmental threats?

- Fire hazards
- Water damage
- Temperature/humidity controls

1-12 List projected technology and application implementations.

Provide a detailed explanation for each of the following questions.

2.0 Network Management

- 2-1 Are corporatewide network security policies and procedures in place related to the physical and logical access controls of the network?
- 2-2 Are corporatewide network security standards maintained?
- 2-3 Do separate operating locations communicate on a regular basis to discuss network issues, operating procedures, modification schedules, and coordinate processing requirements?
- 2-4 Has a risk assessment of the network ever been performed? If so, are copies of the review available?
- 2-5 Is appropriate and updated documentation in place for the planning, design, implementation, and maintenance of the network to include:
 - Hardware and terminal configurations?
 - Subsystem applications?
 - Target performance procedures?
 - Maintenance procedures for:
 - Migration steps?
 - Test plans?
 - Implementation procedures?
 - Security requirements?
- 2-6 How many full-time personnel are responsible for the maintenance of the network?
- 2-7 Identify all remote and local network control terminals and the operations personnel who are authorized to use them.
- 2-8 Are consoles that provide access to the network located in a secure environment?

INFORMATION SECURITY ARCHITECTURE

2-9 Describe the communications planning process.

Who performs the planning process?

Are the plans presented to senior management for review and approval?

Is a strategic plan developed? (obtain and review)

2-10 Has the network design been reviewed for efficiency and to reduce current and future communications expense?

2-11 When was a major reconfiguration or upgrade to the network performed?

2-12 Have communications links throughout the organization been consolidated in the past three years?

2-13 Are there any planned telecommunications or network upgrades or modifications planned?

3.0 Network Access Control

3-1 Who is responsible for placing access controls on the network? Describe their roles.

3-2 Identify the software components of the network that provide log-on security.

3-3 What controls exist to protect the network from external intrusion?

3-4 Does an authorization process exist for all new network connection requests?

3-5 Are assessments conducted of connections to public and third-party networks?

3-6 Do password controls include automatic restrictions on the type of passwords that can be used (for example, length, type of characters, history files, cycle times, lockout for failed log-in attempts)?

3-7 Is a formal procedure in place for requesting access, registering users, and modifying access as required? Describe this procedure and any forms used for the registration process.

3-8 Who typically requests access to the network?

Who authorizes network access requests?

Who performs the modification to access requests?

How are modifications to access documented/retained?

3-9 Is there a formal procedure in place to notify network administrators and resource owners to revoke access when an employee leaves the organization?

3-10 Are reviews conducted on a quarterly basis to validate that user access is appropriate? Describe the mechanism in place that ensures this review takes place.

3-11 Does this periodic review check for inactive accounts and employees who have terminated employment or changed job responsibilities?

3-12 Is a facility used to automatically log users out of the network for system inactivity?

3-13 Are users forced to change their passwords on a monthly basis?

3-14 Are privileged users required to change their passwords more frequently?

3-15 Upon initial log-in, are users forced to change their password immediately?

3-16 Are other forms of authentication used? (check all that apply)

- Single-use passwords _____
- Biometrics _____
- Smart cards _____
- Other _____

3-17 Are passwords encrypted across the network, in stored password files and on backup files?

3-18 Have all default passwords been changed on all network equipment and operating systems (routers, switches, etc.)?

3-19 Is the internal network considered “secure” and are transmissions over the internal network in cleartext?

4.0 Third-Party Service Providers

- 4-1 Is the network maintained by an external network provider?
- 4-2 If so, is a copy of the contract available that describes service-level agreements?
- 4-3 Is an SAS-70 report available on the service provider and if so has it been obtained and reviewed?
- 4-4 Do internal organization personnel have access to view router configurations?
- 4-5 How is the communication of change management performed between network service provider and the organization?
- 4-6 Are unique user IDs and passwords assigned for third-party administrators or is a generic log-in and password used?
- 4-7 Are third-party network providers required to change their passwords according to internal organization password policies?
- 4-8 Is third-party or vendor access controlled by logging all access requirements, resetting passwords, and maintaining audit trails for all maintenance or access?

5.0 Remote Access

- 5-1 For dial-in or remote access, what type of authentication exists?
 - Challenge/response
 - Dialback
 - Other
- 5-2 Describe control mechanisms for remote access? (Check all that apply)
 - Modem only (password and ID)
 - Remote Access Server (RAS)
 - Tokens (dual authentication)
 - Single-use passwords
- 5-3 What functions do dial-up facilities provide? Identify all the uses for dial-up.
- 5-4 Is there a list of authorized users of the dial-up facilities? Does management review this list to ensure that it is current? Ensure that appropriate levels of management review are being conducted.

- 5-5 Is remote access via modem allowed for remote diagnostics and support? (All remote access should be protected with some form of authentication and security control mechanisms.)
- 5-6 Are telephone numbers on modems confidential? Are the numbers unlisted and changed periodically?
- 5-7 Are telephone numbers removed from modems to prevent dial-in?
- 5-8 Does the system disconnect once the transmission is complete?
- 5-9 Are computer system ports that allow dial-up access via public lines limited to specific ports?
- 5-10 Is vendor remote dial-in for diagnostics controlled by requiring the vendor to register with supervisors prior to performing system access?
- 5-11 Are vendors restricted to a callback process controlled by the network staff?
- 5-12 Is a log maintained for dial-in processes that includes time, date, caller ID, and purpose of access? Who maintains this log and who reviews it?
- 5-13 Are users permitted to maintain and use modems connected to their desktops? If yes, is use of desktop modems approved for business use?
- 5-14 Has a modem assessment ever been performed and are network personnel knowledgeable about the number of authorized modems? Is modem use monitored?
- 5-15 What type of remote control software is authorized and used throughout the organization? Is there a policy documented restricting the use of remote control software and modems?

6.0 Hardware/Software/Circuits

- 6-1 How is inter-location compatibility assured?
- 6-2 What actions have been taken to standardize the telecommunications architecture and operations among the multiple processing locations?

INFORMATION SECURITY ARCHITECTURE

- 6-3 Who makes the decisions for the purchase of shared equipment and leased lines?
- 6-4 How are shared equipment and leased lines supported and by whom? How is that support costed?
- 6-5 Are there regularly scheduled meetings to discuss modifications, implementations, and the status of projects? Who attends these meetings?
- 6-6 Is preventative maintenance scheduled for all equipment and is it documented? Is a schedule available for review?
- 6-7 Is there a formal process for changing network control parameters?
- 6-8 How are change requests initiated?
- 6-9 How are changes scheduled and communicated to affected user communities?
- 6-10 Do emergency network changes bypass the change control process? What controls exist to ensure that emergency changes are adequately addressed in the formal change control process and appropriately documented?
- 6-11 Determine if management authorizes the initiation of network acquisitions, configuration modifications, and maintenance.
- 6-12 Define what controls exist to track and report the status of network changes.
- 6-13 Are audit trails of changes available and are they maintained and reviewed?
- 6-14 Determine if there is change request documentation that records the reason for the modification, date of modification, and appropriate approvals.
- 6-15 Is segregation of duties maintained? Is there second-party review of network configurations and changes prior to implementation?
- 6-16 Is adequate documentation of installations and disconnects maintained?

7.0 Backup and Recovery: Adequate controls over backup and recovery should be in place to ensure the resolution of network problems in a timely manner and the resumption of network services within a reasonable amount of time. Alternate paths ensure that network services are uninterrupted.

7-1 Are alternative points of presence available to the building housing processing facilities?

8.0 External Access

8-1 Does the network run TCP/IP?

8-2 Does the network configuration include routers and Ethernet switches?

8-3 Are there direct network connections with third parties (business partners, suppliers, customers, application support vendors)?

8-4 Are third parties permitted dial-in access to the internal network?

9.0 Internet

9-1 Is the internal network directly connected to the network?

9-2 Is there a central point of control for Internet access (firewall, gateway, routers)?

9-3 Are users permitted to use dial-out capabilities from desktop modems to their personal Internet service providers?

9-4 Does an Internet Policy exist that details appropriate authorization and use of Internet services?

9-5 What type of Internet services are provided to users of the organization?

- E-mail
- Telnet
- FTP
- Web searches
- List server services

9-6 Are all employees permitted Internet access or is access approved based on business use only?

9-7 What is the process for approving Internet access to users?

INFORMATION SECURITY ARCHITECTURE

9-8 What kind of traffic is permitted over the Internet gateway?

- | | |
|--|--|
| <input type="checkbox"/> HTTP (hypertext) | <input type="checkbox"/> NTP |
| <input type="checkbox"/> PPTP/VPN | <input type="checkbox"/> NNTP (Net News) |
| <input type="checkbox"/> SHTTP (secure http) | <input type="checkbox"/> POP |
| <input type="checkbox"/> Kerberos | <input type="checkbox"/> Lotus Notes |
| <input type="checkbox"/> FTP (File Transfer Protocol) | <input type="checkbox"/> finger |
| <input type="checkbox"/> TFTP (Trivial File Transfer Protocol) | <input type="checkbox"/> NetBIOS |
| <input type="checkbox"/> Telnet | <input type="checkbox"/> Imap |
| <input type="checkbox"/> Anonymous Telnet | <input type="checkbox"/> SNMP |
| <input type="checkbox"/> SMTP (Simple Mail Transfer Protocol) | <input type="checkbox"/> UUCP |
| <input type="checkbox"/> rsh (remote shell) | <input type="checkbox"/> Netware |
| <input type="checkbox"/> shell | <input type="checkbox"/> Banyan Vines |
| <input type="checkbox"/> rxd | <input type="checkbox"/> Talk |
| <input type="checkbox"/> xauth | <input type="checkbox"/> Domain |
| <input type="checkbox"/> xwindows | <input type="checkbox"/> Name server |
| <input type="checkbox"/> icq | <input type="checkbox"/> Oracle |
| <input type="checkbox"/> ICMP | <input type="checkbox"/> SQL Net |
| <input type="checkbox"/> BGP | <input type="checkbox"/> Remote Connect |
| <input type="checkbox"/> Netview | <input type="checkbox"/> PC Anywhere |
| <input type="checkbox"/> Other _____ | <input type="checkbox"/> Other _____ |
| <input type="checkbox"/> Other _____ | <input type="checkbox"/> Other _____ |
| <input type="checkbox"/> Other _____ | <input type="checkbox"/> Other _____ |

9-9 Does the organization perform content filtering that limits access to certain types of Web sites?

9-10 What type of sites are filtered?

9-11 Are Internet traffic logs maintained and reviewed?

9-12 Are traffic reports published?

9-13 Does the organization have a Web site?

9-14 Is the Web site maintained by a third party or in-house?

9-15 Is the Web site static or are business transactions being processed over the Web site?

9-16 What type of transactions are being processed?

9-17 If transactions are being processed, how are transactions processed through the gateway to production processors?

9-18 How is the Web site's operating system secured?

9-19 How are users/clients authenticated through the Web site?

9-20 Is Web site certification being performed on a periodic basis?

9-21 Is real-time monitoring of the firewall being conducted?

9-22 Does virus software reside on the firewall and is all traffic scanned?

- Inbound only
- Outbound only
- Both directions

Appendix B-4

Windows NT

Assessment

Workplan

WINDOWS NT ASSESSMENT WORKPLAN

Organization: _____

Business Unit: _____

Review Conducted on: _____

Review Conducted by: _____

1.0 SYSTEM CONFIGURATION

- 1.1 Ensure that versions of Windows NT are 3.51 or higher operating systems to take advantage of the security modifications made in later versions.
- 1.2 Ensure that the latest Microsoft service packs and hotfixes for Windows NT have been installed and appropriately configured to take advantage of modifications to errors in the operating system that have been made to new version releases.
- 1.3 Ensure that a procedure exists to receive upgrade, hotfix, and service pack information from MicroSoft or from the MicroSoft Web site. The procedure should include dissemination of hotfix and service pack information to all Windows NT administrators. This responsibility should be defined to a particular individual or group of individuals.
- 1.4 Verify that “system key” options of Service Pack 3 are implemented on all Domain Controllers to enable stronger encryption of the SAM database.
- 1.5 Verify that the Primary Domain Controller (PDC) and Backup Domain Controller (BDC) used for authentication purposes is not

INFORMATION SECURITY ARCHITECTURE

running other applications. PDCs and BDCs used for authentication would be subject to vulnerabilities of the application.

- 1.6 Define an authentication domain for all PDCs and BDCs used as authentication servers to isolate users and the authentication functions. This will increase security and simplify network administration.
- 1.7 Enter user accounts only on the authentication domain and in logical global groups only to ensure central administration and controlled resource allocation.
- 1.8 Ensure that the users' local group contains only the domain users' global group from the authentication domain. Local user groups should not contain any user accounts. No global groups should exist outside of the authentication domains.
- 1.9 Ensure that the built-in Domain Administrators global group of the authentication domain is on every server's Administrators local group.
- 1.10 Ensure that system services are not allowed to "interact with the desktop" when they are started. All services should run under the secured context of a local account, not a global account. Verify settings for "Log On As" in the server manager for each service on each server.
- 1.11 Ensure that the Windows NT screen saver with password protection is utilized on all servers.
- 1.12 Ensure that all system management is performed by using system native tools to ensure that users and directories are established in a secure manner.
- 1.13 Upon system implementation, disable the ability for servers to automatically log on.
- 1.14 System auditing should be enabled for log-on and log-off, and system restart and shutdown. In addition, auditing should be enabled after careful analysis to ensure that only useful and usable information is logged and reviewed. Too often, full logging capabilities provide unusable system logs due to the amount of information that is gathered.

2.0 DISASTER RECOVERY

- 2.1 Redundant user databases should be maintained within each domain to provide load balancing as well as increased recoverability.
- 2.2 Determine if a disaster recovery plan has been documented in accordance with enterprise policies and standards and that it has been periodically tested for effectiveness.
- 2.3 Ensure that Uninterrupted Power Supply (UPS) is available to provide backup capability in emergency situations.

- 2.4 Ensure that a backup emergency disk is available on all Windows NT critical systems. This disk should be maintained in a secure location and possibly off-site to be available if site locations become destroyed or damaged.

3.0 FILE SYSTEM ACCESS

- 3.1 Ensure that the Windows NT File System (NTFS) is used on all partitions on each Windows NT system. NTFS is designed to associate access control to each file or resource. The use of other file systems such as File Allocation Table (FAT) or High Performance File System (HPFS) partitions is not subject to the access control designed into the NTFS. Be sure to convert all FAT and HPFS partitions to NTFS to maintain the security features of this file system.
- 3.2 Check that files requiring different access levels are placed in separate directories. This will ensure that changes to directory permissions apply to the same level of access at the file level contained within the directory. Changes to directory permissions can affect the access permissions of files contained within the directory.
- 3.3 Ensure that data files are in separate directories from executable, batch, and DLL files. Write, delete, and full control permissions should be limited to those individuals responsible for application administration.
- 3.4 Ensure that ACLs for files and directories do not specify individual user accounts or Global Groups, but specify only Local Group access. The Windows NT structure is designed so that users are placed in Local Groups and Global Groups are placed in Local Groups. Only Local Groups are granted rights to resources.

4.0 USER AND GROUP ACCESS

- 4.1 Ensure that the permissions to the special group "Everyone" are appropriate. The special group "Everyone" should have no access to files in application or system directories, shares, and should not have any user rights.
- 4.2 Ensure that access to sensitive system utilities is limited to only those users requiring access to perform a specific and legitimate job function.
- 4.3 Establish one-way trust relationships between resource domains and an authentication domain to establish controlled access of users in the resource domain. The resource domain should have established trust for the authentication domain, and not vice-versa.
- 4.4 Enforce user and workstation time restrictions for standard work-hour arrangements. Ensure that the users are automatically logged off at the expiration of the authorized time.

INFORMATION SECURITY ARCHITECTURE

- 4.5 Define and enforce standard naming conventions for user accounts and groups.
- 4.6 Ensure that standards have been defined and documented for adding, deleting, and modifying users and groups in each domain. Ensure that all users and groups are documented.
- 4.7 Ensure that inactive accounts are disabled after failing to log-on to the authentication domain after a defined period of time.
- 4.8 Ensure that default accounts are renamed immediately upon system implementation.
- 4.9 Disable the guest account immediately upon system implementation.
- 4.10 Disable the ability for anonymous users to access the system. Service Pack 3 provides the capability to restrict this type of access.

5.0 **PASSWORD CONTROL**

- 5.1 Ensure that administrator account password parameters are appropriately stringent in relation to the access levels assigned to the account.
- 5.2 Ensure that the account lockout feature is enabled according to security policies and standards so that failed log-in attempts result in restrictions to the account.
- 5.3 Use 'passfilt' provided in the Service Pack to ensure stringent password controls.
- 5.4 Set password parameters according to security policies and procedures. Password parameters are minimum length, uniqueness, expiration and forced password changes, change password upon initial log-in, cycle time for password reuse.

6.0 **REMOTE ACCESS**

- 6.1 Ensure that remote access to the registry is restricted to only those users requiring access to perform a specific and legitimate job function. Typically, only the system administrator and his or her backup should have this access.
- 6.2 Windows NT Remote Access Servers (RAS) should be configured with minimal protocols and services necessary to implement remote access. User accounts to remote access should be minimal and validated for legitimate business use. One-time password systems should be used in conjunction with the RAS server to minimize the risks associated with remote access.
- 6.3 Ensure that access to the SNMP database is secured and accessible to only administrators requiring access to perform their job function. This database provides access to sensitive network and routing information that could be used to gain access to system resources if available to the wrong persons.

7.0 NETWORKING

- 7.1 Ensure that standard naming conventions are used to provide manageability for the system administration function.
- 7.2 Ensure that domains are established according to defined network procedures. Domains should be appropriately documented. Ensure that domains are defined in lieu of workgroups for authentication purposes.
- 7.3 Separate test and development domains from production domains.
- 7.4 Utilize the resource kit utility 'passprop' to enable the lockout function on the Administrator accounts over the network.
- 7.5 Internet Information Server should be installed, if needed, behind a firewall in accordance with defined security standards and procedures.

Appendix B-5

Telecommunications Security Assessment Workplan

Telecommunications Security Assessment Workplan

Objective: The objective of this review is to ensure that reasonable controls are in place and are effective to ensure the authorized use of voice networking.

1.0 Technology Overview

- 1-1 List switch/key platform and operating system.
- 1-2 List type of equipment used for voice messaging.
- 1-3 List third-party service providers and their functions in installing, maintaining, or responding to emergencies.
- 1-4 List network and equipment administration tools used.

2.0 Organization and Reporting

- 2-1 How many full-time equivalent (FTE) positions exist for the management of the telecommunications function?
- 2-2 Describe the positions and the major responsibilities of each FTE.
- 2-3 Who does the telecommunications department report to?
- 2-4 Are third-party service providers involved in the day-to-day management or on-site management of the telephone cabling or switch? Describe who, when, and how often support is obtained and for what functions.

INFORMATION SECURITY ARCHITECTURE

2-5 Have job descriptions, duties, and responsibilities for the various telecommunications personnel been defined and documented?

3.0 Administration and Management

3-1 Do procedures or standards exist for:

- Approved equipment types (i.e., PBX, key systems, terminals)?
- Authorization procedures for installing new equipment?
- Scheduling procedures for installing lines and terminals outside normal operating hours?
- Operating procedures and telecommunications responsibilities between two connected sites?

3-2 Are all trunks documented and validated on a regular basis? Is wiring appropriately labeled to allow easy identification and efficient performance of maintenance?

3-3 Is documentation on lines, trunks, extension assignments, configurations, etc. stored in a secured environment with limited access? Are outdated documentation and phone lists/books destroyed appropriately?

3-4 Are switch reports, logs, and call detail handled as sensitive information with appropriate storage, distribution, and destruction instructions?

3-5 Are wiring closets, the Main Distribution Facility (MDF), the Intermediate Distribution Facility (IDF), and telecommunications equipment areas locked at all times?

3-6 Is access to these areas restricted and controlled to allow only individuals with direct responsibility for the maintenance of these facilities?

3-7 Is there a list that documents authorized individuals to these facilities? Are logs maintained on daily access to include date, time of entry, time of exit, purpose of access, name, and contact information of individual granted access?

3-8 Are environmental controls commensurate with the requirements of the equipment? Do controls exist for fire, flood, and extreme temperature changes?

3-9 Are contract agreements available for PBX services? Do contracts exist for local exchange carriers (LECs), long-distance carriers, PBX vendor support, voicemail systems, and automated attendant systems?

- 3-10 Has user awareness and training been established to include proper use of the phone system? Does training include awareness on how to recognize and report indications of telecommunications fraud? Does training awareness include end-user telephone system security responsibilities?
- 3-11 How are telecommunications issues logged and tracked?
- 3-12 Is there an operational recovery plan for the PBX, voice messaging, voice response, and automated attendant systems? Are the plans tested annually?
- 3-13 Is a contact sheet available listing individuals to contact for 24-hour support or reporting?
- 3-14 Is a Toll Fraud Recovery Plan documented and reviewed?
- 3-15 Are there two separate points of presence into the MDF and are the cables run by two different service providers?

4.0 Technical Assessment

- 4-1 Have all default passwords been changed on switches, voice messaging systems, interactive voice response systems, and automated attendant systems? Are passwords in compliance with password policy for all other computing systems? Are passwords changed monthly?
- 4-2 Is maintenance port password administration in compliance with password policies? Are maintenance port passwords changed monthly?
- 4-3 Has Class-of-Service (COS) and Class-of-Restriction (COR) been assigned to incoming facilities, station users, authorization codes, ports, and modem pools?
- 4-4 Has direct access to trunks and trunk groups been restricted?
- 4-5 Has remote access or Direct Inward System Access (DISA) been restricted or disabled?
- 4-6 Has the ability to dial out from voice messaging or automated attendant systems been disabled? Restrict transfer capabilities to within the PBX.
- 4-7 Has the ability of incoming calls to access outgoing trunk groups been restricted?

INFORMATION SECURITY ARCHITECTURE

- 4-8 Are international dialing capabilities restricted to only those countries in which the organization operates?
- 4-9 Are time of day and weekend access restrictions in force?
- 4-10 Has the ability to place long-distance calls been restricted or disabled?
- 4-11 How often are PBX, voice messaging, interactive voice response systems, and automated attendant system options monitored and checked for appropriateness?
- 4-12 What type of call detail information is being captured?
(check all that apply)
- | | | | |
|-------------------------------|--|---|-------------------------------|
| <input type="checkbox"/> Date | <input type="checkbox"/> Origination of call | <input type="checkbox"/> Extension | <input type="checkbox"/> Cost |
| <input type="checkbox"/> Time | <input type="checkbox"/> Destination of call | <input type="checkbox"/> Length of call | |
- 4-13 Are fraud monitoring and alert processes in place? Are these processes contracted by third-party service providers?
- | |
|--|
| <input type="checkbox"/> Real-time call detail report (CDR) exception analysis |
| <input type="checkbox"/> Carrier alert services |
| <input type="checkbox"/> Other |
- 4-14 Are phone bills reconciled to call detail reports (CDRs) on a monthly basis?
- 4-15 Are CDRs reviewed internally for fraud and abuse?
- 4-16 Are phone bills separated by business unit or department for management review and validation of reasonableness?
- 4-17 Are call statistics analyzed over time to determine trends and establish statistical baselines for comparison? Are histograms prepared and analyzed?
- 4-18 Are reports run on calls exceeding a certain time (i.e., 15 minutes)?
- 4-19 How often are status logs for voicemail reviewed?
- 4-20 Are voicemail usage reports reviewed?

Appendix C-1

Computer Incident/Emergency Response Plan

1.0 OVERVIEW

This plan is designed to provide the capability to respond to computer security incidences in a timely and coordinated manner to reduce their impact on the effectiveness of systems internal to the organization. Its implementation will contribute to the improvement of computer security and will be used to provide input to the modification of policies regarding computer use and misuse.

The organization's processing environment is a target for malicious and criminal activity and damage caused by curious users and accidental mishaps. Damage can be caused by computer viruses, sabotage, break-ins, theft of information, covert monitoring (sniffing), modification or destruction of data and software, spamming, or failure to execute proper security procedures such as daily backups.

The objective of this plan is to:

- Enhance the security of all systems within the organization
- Standardize the response to security issues, thereby increasing the effectiveness of communication throughout the organization, reducing the amount of damage that occurs during an incident, and resuming normal business processes rapidly
- Provide defined points of contact throughout the organization to speed communication and response time
- Provide the mechanism for collection and dissemination of security-related issues
- Coordinate the use of resources for responding to incidences
- Provide for overall awareness of potential threats, risks, and security in the computing environment
- Prevent known incidences from reoccurring

2.0 THE PLANNING PROCESS — *Creating the plan so that it is easily understood and implemented is critical.*

Planning includes the following considerations:

- Involve all departments and personnel that will play a role in the response effort to ensure an adequate understanding of the plan.
- Incident and emergency response priorities must coincide with the organization's policies, business goals, and objectives.
- Develop plausible scenarios related to the realistic risk to assist with the development of possible solutions.
- Training is essential, as well as testing of the plan for effectiveness.

3.0 ORGANIZATION — *The following individuals make up the ALERT. ALERT is the acronym for the team of individuals that will respond, assist, and support the incident recovery efforts. ALERT stands for:*

Assistance (and)
Leadership (for)
Emergency
Response
Teaming

Members of the ALERT team will consist of Corporate Information Security, security liaisons/coordinators, application coordinator(s) for the affected system(s), help desk, and designated executive management. Responsibilities include:

Information Security Organization:

- Security policy and awareness training development
- Develop and maintain the Computer Emergency/Incident Response Plan
- Train, organize, and coordinate the ALERT
- Provide leadership for solution determination, recovery, and investigation of all incidences
- Coordinate external support in response to ALERT efforts
- Assign an ALERT coordinator for each incident to manage the investigation, follow-up, and closure of the incident in a complete and timely manner
- Review security alerts published by other professional security organizations

ALERT Team:

- Assist in solution determination, recovery, and investigation of all incidences

- Make all necessary corrections to system and components to ensure that vulnerabilities are eliminated/reduced and to ensure non-reoccurrence of the incident
- Test modifications for effectiveness
- Communicate with management regarding incident reporting, status updates, and investigation results; communicate all modifications to systems and components and status of vulnerabilities
- Document the incident to include problem statement, analysis, resolution, and control implementation
- Conduct a post-incident review and incorporate incident “lessons learned” in Security Awareness and Training Program

4.0 NOTIFICATION PROCESS

The notification process for a security incident or emergency should be known throughout the organization. The notification process should be a topic for the Information Security Awareness Program so that all individuals and computer users in the organization are knowledgeable of who to turn to immediately when a suspected incident is occurring or has occurred. There should be no question of who should be the first number dialed or where to find that number.

The notification process may consist of contacting the help desk when a help desk is available to the organization. This facilitates the automated logging of the incident and the identification of the correct response procedures, as well as the phone numbers of emergency contacts. If a help desk is available, it would be considered the first level of response and it is critical that help desk personnel understand their very vital next steps.

If a help desk is not available, a primary point of contact is necessary to start the ALERT actions. The primary point of contact may be the Information Security Officer. The first individual contacted is responsible for the notification of the ALERT team and all individuals on the notification roster. These individuals should assemble immediately to begin information gathering and take the necessary steps to minimize damage to the organization.

Another consideration in the notification process is to contact management personnel within the area or department of the suspected compromise as well as executive-level management. These individuals do not necessarily need to be members of ALERT but should understand the status of events and be given the consideration for status updates and resolution.

5.0 EMERGENCY RESPONSE POINTS OF CONTACT — *Document name and phone numbers of responsible individuals.*

- Help desk
- Security Officer
- Virus Coordinator
- Chief Information Officer
- Security Liaisons/Coordinators
- Component Administrators/Coordinators
- Vendor POC list
- External Emergency Response Vendors/Consultants

6.0 EMERGENCY RESPONSE PROCESS AND REPORTING CHECKLIST

- Report Problem.
- Establish initial documentation using the Incident Reporting Form.
- Contact first line of assistance (help desk or Information Security Officer).
- Execute the notification roster and establish meeting details for ALERT.
- ALERT begins analysis and information-gathering to determine the extent of the incident, category, and level of severity. Categories may include:
 - Virus
 - Suspicious probe
 - Denial-of-service attack
 - External network penetration
 - Internal network penetration
- Determine if external assistance and support is needed for further analysis and determination of damage or procedures to rectify the vulnerabilities.
- Provide periodic status updates to management.
- Determine steps to resume normal business processes and restore systems.
- Develop and implement action plan.
- Test that the solution implementation has reduced or eliminated the vulnerability.
- Continue documentation of the cause of the incident.
- Determine next steps to minimize the risk of the event reoccurring.
- Document all actions taken and submit reports through appropriate communications channels for review, response, and approval.
- Conduct a post-incident review to ensure appropriate communication throughout the organization and integrate findings into other programs such as awareness and training or policies, standards, and procedures modification.

- Continue to monitor the area of vulnerability for signs of weakness and effectiveness of the solution.
- Close out incident.

7.0 INCIDENT REPORTING CHECKLIST

8.0 NOTIFICATION FORM

A notification form provides initial information regarding the perceived incident. Notification forms should be maintained to develop statistics and assist in identifying vulnerabilities within the organization. A sample notification form is as follows.

INCIDENT REPORTING FORM

1. Contact Information

Name:

E-mail Address:

Telephone Number:

Business Unit Location:

2. Affected Components

Component 1:

Host Name:

IP Address:

Function/Application:

Component 2:

Host Name:

IP Address:

Function/Application:

Component 3:

Host Name:

IP Address:

Function/Application:

Component 4:

Host Name:

IP Address:

Function/Application:

3. Source(s) of Attack

- a. Is the intrusion external to the perimeter network? (yes/no)
- b. Has there been an attack on the infrastructure of the network? (yes/no)
- c. Has the intruder gained the supervisor or root password to the systems listed above? (yes/no)

List which systems:

- d. Has the source of the attack been identified? (yes/no)

Host Name:

IP Address:

- e. Has contact with the perpetrator been made? (yes/no)

Explanation _____

4. Description of Attack

Include dates, methods of intrusion, intruder tools involved, software versions and patch levels, intruder tool output, details of vulnerabilities exploited, source of attack, or any other relevant information.

- a. Are you aware of any exploit scripts or tools in your system that have been left by the intruder?
- b. Are you aware that any exploited passwords are being used?

Appendix C-2 Sample Line of Business Security Plan

**Information Security Architecture
Line of Business Security Plan
at
Starcross, Inc.
April 20, 2000**

Contents

Executive Summary	
LAN Assessments	
LAN/WAN Gateway Review	
Internet Review.....	
Routers	
Pix Firewall	
UNIX Server.....	
Conclusion.....	
Glossary of Terms	

EXECUTIVE SUMMARY

Background

Starcross wants to ensure security of its information assets by providing appropriate levels of control for all components of the Starcross processing environment. As Starcross continues to grow, and finds new ways to serve its customers, state-of-the-art technology is deployed as an enabler to meet Starcross' business goals. However, with the enhanced capabilities of this new technology come increased vulnerabilities. By their nature, technologies such as wide area networks (WANs), local area networks (LANs), personal computers (PCs), and Internet connections increase the risk of unauthorized access and wrongful disclosure of sensitive information.

Starcross has reviewed and assessed the risks related to their LAN, WAN, and the related network access points into its processing environment. The risks, vulnerabilities, and controls have been identified in this document as well as documented discussion of the actions necessary to improve controls and decrease risk. Starcross management is aware of the need for consistent information security policies and standards across all of the information system (IS) technologies that Starcross relies on to serve its customers.

This Security Plan focuses on certain components of Starcross' IT processing environment and efforts needed to establish the fundamental security attributes for protecting Starcross' critical information: confidentiality, integrity, and availability. The Security Plan focuses on the wide and local area networks and their interfaces to the processing environment and an assessment of Netware servers, Windows NT servers, and UNIX servers. The procedures performed include evaluation and documentation of the adequacy of established controls, identified control issues and related business risks, and provided recommendations to strengthen current controls.

LAN Assessments

Netware assessments were performed using the Bindview automated assessment tool to analyze system parameters, access rights, and resource utilization information. These assessments were performed on the LANs housing the Accounting and Commercial Lending applications. A general controls review of the LANs included an assessment of LAN policies, standards and procedures, logical access to Netware server resources, security parameters, and management controls.

During the review, inconsistencies related to the administration of the LAN environments were noted. The recommendations in this Security Plan should be implemented to enhance the LAN environment at Starcross.

LAN/WAN Gateway Review

The connectivity assessments performed on intranet gateways and LAN segmentation focus on controls implemented to restrict access across network segments and between business units and departments via the intranet. This included an assessment of physical and logical segmentation of the network, and the use of switches, bridges, and routers. In addition, external connections to the operating environment via remote access, EDI, and Internet connectivity have been evaluated.

Internet Review

The technical assessment of the Internet included a review of the network schematics and current configurations of firewalls, routers, gateways, Internet services, proxy servers, and authentication and filtering mechanisms. Starcross has a high level of awareness for security throughout the organization. Assessments of the Internet application, from user interface to the application engine housed on an Edify server, have been determined to be appropriately designed from a control perspective.

The objective of Starcross IT projects is to build in a reasonable level of security that appropriately corresponds to the level of business risk related to the transactions and information being processed. Business risk is a key driver in determining the level and type of controls that have been, or will be, implemented.

Internet control issues noted are related to informal procedures, increased access capabilities, and lack of documentation. While these control issues represent potential increased internal control risk to Starcross, these risks are understood and have been accepted by senior Starcross management. IT management is aware of many of the issues noted and is currently addressing those issues to bring the Internet environment to the same level of control as found in Starcross' mainframe environment.

Conclusion

Starcross management is aware of the importance of information security. Overall, Starcross has made the investment in skilled IT professionals and leading technology to allow Starcross to compete in the aggressively changing manufacturing industry. Starcross' rapid growth and acquisition of multiple network and processing platforms has resulted in resource constraints in managing those homogeneous platform and network components in a controlled and integrated manner.

The issues detailed in the document have been incorporated into the action plans of both the IS Organization as well as the Security Steering Committee.

INFORMATION SECURITY ARCHITECTURE

Consistent application and enforcement of information security policies, standards, and procedures is an objective of both Starcross IT management and executive management. Related to this goal, efforts have started to better understand how the control objectives present in the mainframe environment can be achieved for the distributed processing environments.

As noted by IT management, a security infrastructure is under development that defines the decentralized roles for security and supports the requirement for appropriate resources, time, and personnel. In January 1999, an Information Security Policy was developed. This policy required approval and support from all departmental and business unit managers to ensure that the objectives could be met. Using this policy as the foundation, organizationwide security standards and objectives are being created, approved, communicated, and supported. Once the policy, standards, and objectives are in place, security baselining for all components (databases, operating systems, networks, applications) will be performed by the designated security administrator for that component. These baselines will be merged with best practices to establish specific procedures for each component that support the security objectives and standards.

Implementation of the identified recommendations, further definition and support of a security infrastructure, development and approval of a Security Policy, baselining security for all components, and development of an SS&PM will allow Starcross to continue to refine its Information Security Architecture.

NOTE: In the interest of avoiding disclosure related to Starcross' proprietary systems and methodologies, certain descriptive information, related to system component background and strengths, has been omitted from this document.

LAN ASSESSMENTS

Overview

A series of Netware assessments were performed using the Bindview automated assessment tool to analyze system parameters, access rights, and resource utilization information. These assessments were performed on the LANs housing the General Ledger and inventory applications. A general controls review of the LANs included an assessment of LAN policies, standards and procedures, logical access to Netware server resources, security parameters, and management controls.

Methodology

The methodology for these assessments included an interview with each of the LAN administrators to discuss general controls. These interviews

were supplemented with the execution of Bindview ESM. The scope for Novell 3.x included:

- Bindery Listing of Objects and Security Equivalencies
- Users with Sensitive System Directory Access:
 - SYS:SYSTEM
 - SYS:LOGIN
 - SYS:PUBLIC
 - SYS:MAIL
- All of the Volumes with Related Information
- Users with ADMIN Equivalency or Supervisory Rights
- Password Parameters
- Intruder Detection Information
- User Listing
- Group Listing
- Time Restrictions

The scope for Novell 4.x included:

- A Listing of NDS Objects and Security Equivalencies
- Users with Sensitive System Directory Access:
 - SYS:SYSTEM
 - SYS:LOGIN
 - SYS:PUBLIC
 - SYS:MAIL
- All of the Containers with Related Information
- Users with ADMIN Equivalency or Supervisory Rights
- Password Parameters
- Intruder Detection Information
- User Listing
- Group Listing
- File and Print Server Listing
- Invisible Objects Listing
- NLM and Replica Listing

General Ledger LAN

The GL local area network (LAN) is a computer-based account processing and reporting system that provides tracking, analysis, and input of accounting information by employing personal computer workstations connected to the LAN. The LAN allows personal computers to share accounting information, software, disk drives, printers, and other peripherals.

The LAN administrator for this LAN is Ben Lowery, Director of Accounting. Mr. Lowery has strong technical competence and a sufficient awareness of the importance of security over the network. The queries produced by Bindview were evidence that this LAN has sufficient controls in place and

INFORMATION SECURITY ARCHITECTURE

is operating in a secure, effective environment. The LAN administrator has also created an overall awareness of security to the users of this network.

Commercial Loan LAN

The MP-100 Risk Processor is a client/server system that evaluates credit requests for one or multiple products using criteria specific to each product. The system maintains decision strategies for up credit products or market segments and applies decision criteria to each. A multi-tiered strategy is employed to assess credit risks. The system matches the selected strategy to each lending scenario.

The LAN administrator for Commercial Loan is Scot Damian, Assistant Vice President of Commercial Loans. Mr. Damian is the Chair for the LAN Administrator Group, which is a segment of the PC Committee, and is also responsible for administration of the Intel virus software signature files and upgrades for all Novell networks. He is very technically competent and keeps abreast of new technology, network operating system upgrades, and network and security issues, in addition to his other responsibilities within Starcross. Procedures documentation has been and is comprehensive and complete.

The queries produced by Bindview were evidence that this LAN has sufficient controls in place and is operating in a secure, effective environment. Mr. Damian has also created an overall awareness of security to the users of these networks as well as the members of the LAN Administrator Group.

The following management control issues have been identified for improvement and relate to the administration of the networks listed above unless specifically stated.

Report of Issues

The intent of these assessments was to document and evaluate the adequacy of established controls, identify weaknesses and related business risks, and provide recommendations to strengthen current controls. The following list of concerns have been communicated to those individuals responsible for the maintenance and administration of the LANs.

LAN Administration

The LAN administrators responsible for the three LANs under review have a high level of security awareness and have strong technical skills for the maintenance and administration of these LANs. The practices that they use for executing their responsibilities as LAN administrators should be developed into standards and procedures for LAN administration and security.

LAN administration is currently a decentralized function and the majority of administrators hold other primary responsibilities in addition to administering

the LAN(s). Many of the administrators are not given the time necessary to succeed at proper LAN administration, which includes developing and documenting LAN procedures, maintaining appropriate user access, enforcing security requirements, performing backups, implementing the proper tree structure and naming conventions of the network, and understanding changing technology (i.e., migration from Novell 3.x to Novell 4.x). The necessity to stay current with security issues, virus upgrades, and user access, as well as receiving appropriate training, places a significant burden on those individuals who do not have a network background or are expected to juggle all roles efficiently and effectively. The back-office LANs are particularly complex and consist of heterogeneous platforms, a growing number of users, and connectivity to third-party processors.

Suggested Action: It is recommended that consideration be given to move toward a smaller group of well-trained individuals that can manage cross-departmental LANs on the back-office side. For this group, LAN administration should be considered their primary function or full-time position.

Action Taken:

Network Standards and Procedures

While no formal network policies and procedures are addressed in the PC Manual, the manual does state that User Departments are responsible for developing and implementing departmental procedures to comply with the policies defined in the PC Manual. Network procedures were reviewed for both the Accounting and Commercial Lending LANs. These LANs are administered by Scot Damian, who has made a significant effort to document detailed and usable procedures for the administration of the three Novell LANs for which he has responsibility.

Best practices and those procedures already developed at Starcross, are being leveraged to other areas of the company and will become network operating system standards. Each LAN administrator may fall under the direction of different departments, making it difficult to enforce standards under this structure.

Suggested Action: It is recommended that the responsibilities of the LAN Administrator Group be formally defined into a charter and be expanded to include the development of standards and procedures for networks. The LAN Administrator Group is made up of power users and Network Administrators, and is currently designed to coalesce and share information on best practices; however, no management authority exists to develop, approve, and enforce those standards. It is recommended that a central authority, such as the chairman of the LAN Administrator Group, be given that authority to not only provide guidance but also enforce the standards,

INFORMATION SECURITY ARCHITECTURE

procedures, and policies for the network. Per IT management, efforts are currently being made to implement such recommendations.

Action Taken:

LAN Recovery

Detailed recovery procedures exist for the General Ledger LAN and a total LAN restore has been performed. Recovery procedures are designed to reinstall effectively on the backup alternatives available.

Suggested Action: Full-scale tests of disaster recovery plans will continue to be performed on an annual basis to determine whether the most critical applications can be restored within an acceptable timeframe, whether the appointed backup hardware has sufficient capacity for the software, and whether the identified individuals responsible for recovery are sufficient in number with correct responsibilities assigned to them, and with no overlapping, time-consuming responsibilities assigned to any one individual. Plans are being developed and incorporated for each LAN into the company's plan to restore processing in the event of a localized (or site) disaster. The plans are tested at least annually.

The requirement for a backup LAN for this application is being discussed by appropriate management. It is recommended that equipment be identified and designated for recovery operations. In addition, a DOS boot diskette should be maintained off-site with backup tapes to facilitate restore procedures. This is not currently done.

Action Taken:

Novell 3.x to 4.x Migration Strategy

Although Novell is the vendor for both Netware 3.x and 4.x, these two network operating systems are significantly different. Moving from version 3.x to 4.x is more than an upgrade. It requires a migration strategy that includes training for the administrators of these systems. The major differences between the operating systems include a move from bindery files that contain user profiles and security information in the 3.x version, to a centralized Network Directory Structure (NDS) in the Netware 4.x version. The bindery files must be loaded on each server a user is permitted to access in the network. With Netware 4.x, the NDS is located on a primary and backup server, and centralizes the administration of user profile, access, and security parameters.

Suggested Action: Scot Damian has migrated his networks and has documented this migration strategy in his procedures documents. These procedures will be used throughout Starcross, Inc., as a standard for Novell migration.

Action Taken:

Site Licenses versus Individual Copies

Starcross, Inc., currently maintains individual copies of software throughout the company, which requires each copy to be properly registered.

Suggested Action: IT management has stated that in the past, site licenses have been considered and were not cost-effective. However, going forward, management will continue to consider the use of site licenses for standard software throughout the company. A site license can decrease the cost to the company as well as the management and inventory of licenses. One copy of the software can be maintained on a single server with the number of individuals accessing that software controlled by the site license agreement. Site licenses provide a more efficient and effective means of upgrading software as well as maintaining software inventories, reducing disk space on PCs, and minimizing software maintenance requirements for network administrators.

Action Taken:

Automated Tools

The use of automated tools such as Bindview and Auditware can make the execution of a LAN administrator's responsibilities more effective by making documentation efficient and minimizing the risk of inappropriate access rights granted to users that can be verified and monitored through automated reporting. Additionally, Bindview's NetInventory module can be used to automate the task of producing an application inventory of products installed on OS/2 workstations.

Suggested Action: Automated assessment tools and appropriate training should be provided to both LAN administrators and Internal Audit personnel to ensure that access rights, security parameters, and file structures are appropriately configured and can be monitored for compliance.

Action Taken:

Virus Protection

The two virus software packages used at Starcross are LANDesk Virus Protect v3.01 from Intel and IBM AntiVirus. Scot Damian is responsible for

INFORMATION SECURITY ARCHITECTURE

downloading signature files from Intel's Web page and distributing this software to the appropriate LAN administrators and respective servers. LANDesk procedures have been distributed to the LAN administrators of those servers. The procedures used for LANDesk are not consistent with those used on IBM AntiVirus. No documented procedures for maintenance and use of the IBM AntiVirus software within Starcross exist.

Suggested Action: Written procedures should define the LAN administrator's responsibilities related to virus protection, software implementation, upgrades; and use of signature files should be documented and available in a Security Standards and Procedures Document. These procedures should direct the LAN administrator on how to obtain and load signature files, and the frequency and types of files to be scanned. Although two software packages are used, procedures on use should be consistent between the two packages. It should be noted that efforts related to companywide virus protection standards have begun.

Action Taken:

Change Management

The change control policy is not being followed for operating system and application upgrade testing on the Accounting and Commercial Lending LANs. The policy as written includes sign-off from departments and representatives who are either not impacted by the change or do not understand the system being modified. This has previously caused an inefficiency in following this policy for change management due to the lack of participation in sign-off from the required individuals listed in the Policy Manual.

The LAN administrators are responsible for developing procedures related to their departments and local networks. The Policy Manual directs the LAN administrators to develop procedures.

Suggested Action: It is recommended that the procedures developed by those LAN administrators be used to effect change management in their area and relating to LAN technology. These procedures for testing and verification, as already written, should be reviewed for standardization throughout all LANs at Starcross, Inc.

Action Taken:

LAN/WAN GATEWAY REVIEW

Overview

The connectivity assessment for intranet gateways and LAN segmentation focused on controls implemented to restrict access across network segments

and between business units and departments via the intranet. This included an assessment of physical and logical segmentation of the network, and the use of switches, bridges, and routers. In addition, the access points into the processing environment were reviewed. This included the assessment of remote access, EDI, Internet, and e-mail.

The current WAN connects both Ethernet and Token-Ring LANs at two New Jersey locations with five locations throughout the United States. Connectivity between the five national locations include T-1 and fractional T-1 AT&T Frame Relay. X.25 connectivity is used to locations in Egypt, Germany, Sweden, Italy, and France. The X.25 connectivity is being replaced by contracted services with the IBM Global Network. A local microwave link between the two New Jersey facilities provides DS3 throughput. The microwave operates in the 18-Gigahertz range.

The WAN consists of Frame Relay in the New Jersey 1 location, and DDS (channelized T1) circuits in the New Jersey 2 location. T1 links connect the Location 1 router to the Frame Relay cloud. Channelized T1 connects Site A to the Site B router and Data Center.

There are two types of LANs at Starcross: Novell (both Netware 3.x and 4.x) for backoff systems, and OS/2 at branches. A Novell SAA gateway performs protocol conversion at the host for the back-office LANs.

Methodology

A review of the Internet has been performed as well as a review of additional components related to Starcross network access points. For each component and its connectivity, the path analysis included identification of points of access authentication, authorization, administration, as well as monitoring and reporting. The following areas were reviewed:

- Dial-in and Dial-out Access
- External Connections
- Network Security Features
- Wide and Local Area Network Gateways
- Gateway Controls
- Gateway Maintenance Procedures
- Threats to Gateway Implementation
- Effectiveness of Gateway Controls
- Connections to Business Partner Networks
- Risk Associated with Peer Connections
- Network Resources Used
- Controls Available to Support Security and Confidentiality Requirements
- Other Means Available to Support Security Requirements
- Physical Risk

Strengths

Security Release Monitoring. Many individuals at Starcross have indicated that they review Web pages, news groups, and publications for security issues and methods for exploiting security and for new mechanisms of securing network and processing components. In such a dynamic environment, it is crucial that key security-related resources are monitored on an ongoing basis.

Suggested Action: This practice should continue and be formalized to distribute the information to all individuals responsible for security so that they will gain the full benefit from the research being conducted throughout Starcross. The following list is recommended for periodic review:

- <http://coast.ns.purdue.edu> — several freeware security tools
- www.security — how to build a secure WWW connection
- Computer Emergency Response Team (CERT) advisories
- Computer Security Institute newsletters and publications
- Vendor patch releases and updates

Action Taken:

Report of Issues

Physical Security. Invalid access attempts are sent to physical security guards at Site A and Site B locations.

Classification of Sensitive Resources. An informal classification methodology exists and has been described throughout the Policy Manual. This methodology defines two classes of computers: Class I and Class II. Class I computers are significant enough to pose a risk to Starcross because they support production applications, provide remote access connectivity, or act as a shared resource. Class I computers are required to have access security software to limit use to authorized individuals. Class II computers appear not to pose a risk to Starcross' operating environment. This classification of computers can be used as the definition of a formal classification methodology that serves to identify risk with all information assets.

The Policy Manual also defines production application/mission critical as an application that affects the customer's account record, account balance, interest rate, and name and address. Name and address are included because they are used as a compensating control in such procedures as reissuing passwords for the E-commerce applications. The definition of production in the manual includes applications that are mission critical and will update or modify the master files of non-customer financial systems.

Suggested Action: Management should consider if these definitions should be applied to information processing resources and documented in a formal classification matrix.

Action Taken:

Sensitive Data Transfer

A procedure exists for the review of all data transferred across the LANs, to the mainframe or any third party for processing. A form, Request for Data Transfer Authorization, is used for this request. The components of a good classification methodology exist at Starcross.

Suggested Action: These definitions and forms should be consolidated into a methodology that documents classification procedures of sensitive resources and information, access levels to what has been identified as sensitive, and protection mechanisms for each level of classification. A review mechanism should also be in place to ensure that the classifications are current and consistent and that controls or procedures for protection are being enforced.

Action Taken:

Approved Software

Policies and procedures do not exist to facilitate a process for reviewing that only authorized software is run on PCs. Users could be downloading or buying programs to run on their computers that have not been formally approved by Starcross.

Suggested Action: Recommend periodic scans of user computers for unlicensed, unknown software. This can be accomplished by utilizing scanning software such as Bindview NetInventory Module (the NetInventory module can be used to automate the task of producing an application inventory of products installed on OS/2 workstations).

Action Taken:

Data/Resource Ownership

The identification of security owners and security liaisons needs to be documented by position. This can be best accomplished if security responsibilities are written into job plans so those individuals can be measured on their performance and given credit for the extra responsibility.

INFORMATION SECURITY ARCHITECTURE

Starcross has documented a list of security owners by virtue of their responsibilities as stated in the interviews conducted throughout this project. This document can be used as the basis for defining data/resource ownership within the Security Standards and Procedures Manual. For the networks, security at Starcross is a decentralized function. Integration between security responsibilities is not yet seamless and efficient.

Suggested Action: Integrated security administration can be accomplished by defining each of the security administrator/owner/liaison responsibilities and interaction with each other related to an application, network group, and department. We recommend the use of an appendix to the Security Procedures and Standards Manual that documents these positions, responsibilities, and names of the individuals within those positions.

Action Taken:

Security Infrastructure

An infrastructure must be developed to support the continuation of security architecture implementation. This infrastructure should include:

- Definition of the approval authority (Security Committee) for all policies and resolution of security issues
- Development of a Security Team for the development, implementation, and dissemination of security procedures and standards
- Semiannual meetings of all persons responsible for security, which includes security liaisons, Security Team members, and the approval authority

Action Taken:

Confidentiality Agreement

The Starcross Confidentiality Agreement dated November 1999 defines proprietary information, explains nondisclosure of information and the surrender of rights to all Starcross information upon termination of employment, and is primarily directed at inventions and discoveries. The contract contains specific reference to consequences that can be taken if the contract is broken.

The Confidentiality Agreement is required for all employees and is a part of the New Employee Orientation Checklist. This agreement is not oriented toward the computing environment and does not include the protection and use of passwords, appropriate access to files and information, and appropriate use of computer resources.

Suggested Action: These IT-related issues could be included in the current Confidentiality Agreement; however, it is recommended that they be a separate and short document that focuses on the operating environment and computer resources. This document should also specifically state the potential penalties for violations. It is recommended that this document be initiated as a part of the New Employee Orientation Checklist and be signed annually during user awareness training.

Action Taken:

Electronic Mail

No official electronic mail policies and procedures were evident. This includes Novell Mail available at limited locations, and any Internet mail service individuals are using through their Internet service provider (ISP). Attachments are the biggest concern because they can include binary files that can contain viruses. There are no restrictions on e-mail attachments, including size of the attachment, compression before sending, or scanning for viruses before accessing. Starcross' Novell Mail does not currently allow for Internet mail to reach Starcross employees.

Suggested Action: An e-mail policy/guidelines needs to continue to be established/refined to inform users of appropriate use of this service.

Action Taken:

Remote Access

Remote access at Starcross is predominately used by administrators for the maintenance of applications or LANs. The primary control being used is that modems are powered on when needed and powered off after use. The reliance on nontechnical individuals, especially at branches, to power off modems after use should be improved with additional compensating controls. For vendor access, it was indicated that the connection is monitored while the vendor is in the system. Remote access software currently used for applications are PCAnywhere, Carbon Copy, and Close Up. A TACAS server is being considered for centralizing access to routers, but is not currently being used. It was indicated that this is available under the current Cisco contract.

There is currently no policy that restricts the use of modems from desktops. The most significant threat of dial-in and dial-out access to desktops is circumventing the use of virus detection software on any incoming files. Although there are policies related to the use of virus detection software, the use of modems increases the risk of infection. A second threat is that if the modem and desktop PC are not turned off and the desktop contains any

INFORMATION SECURITY ARCHITECTURE

type of server software, this creates an access point into the Starcross, Inc., internal network.

Unfortunately, the only controls that can be put in place for desktop modem usage are detective and administrative in nature. A policy needs to be written to restrict the use of modem usage on Starcross, Inc., desktops. Internet access should also be restricted to the Starcross, Inc., Internet gateway, eliminating individual use of other ISPs such as America Online. This will minimize the threat of viruses and provide the capability to monitor Internet sessions and activity.

The only detective controls for modem usage are reports available from Centrex that will indicate data traffic from modem usage. These reports are not currently received by Starcross, Inc., but could be used to monitor and enforce a policy on modem usage. However, the cost/benefit of receiving and reviewing these reports should be considered.

Suggested Action: As Starcross begins to rely more heavily on dial access to provide enhanced customer support, and to enable greater employee access to information and information services, a consistent security strategy will need to be developed. This strategy should involve:

- Establishing a boundary between internal and external networks
- Defining a consistent access architecture across the enterprise
- Implementing effective monitoring and management reporting mechanisms
- Developing an emergency response capability

To provide a more consistent level of security, controls need to be placed at the boundary between the external and internal networks. Because the potential for compromise is higher when controls are weak, boundary point controls should effectively restrict unauthorized access. Because no control can be absolute, management and audit reporting capabilities should also be provided. Monitoring at boundary points in the network should be focused on detecting conditions that could indicate an attempt to compromise the network or successful access to the network by unauthorized persons.

One-time passwords provide a high level of authentication. Authentication through this method is either by hard tokens (password generator carried by user) or soft tokens (password generator provided on client computer). After being authenticated, users have access to the resources that management has approved by routing them to the specific server based on their user identifier and application.

Enhanced administration and management reporting can be provided through security servers that are used to assign access permissions for individual users, including customers and employees. Authorization controls can be implemented by providing routers to restrict users' ability to freely navigate the internal network.

For added functionality, and to reduce the number of internal log-on identifiers and passwords, a standards-based authentication system can be added to the dial access architecture to provide a single point of administration and authentication. This server will also provide secure authentication between independent systems in particular in distributed or client/server environments. A standards-based approach to authentication is preferable in a heterogeneous environment because vendors have committed to providing the interface as their technology evolves.

Action Taken:

INTERNET REVIEW

Overview

The technical assessment of the Internet included a review of the network schematics and current configurations of firewalls, routers, gateways, Internet services, proxy servers, and authentication and filtering mechanisms.

As part of the Internet review, detailed testing of the TCP/IP network, UNIX server, and configuration of Checkpoint Firewall-1 software was performed using the automated tool Internet Security Scanner (ISS). The tool interrogated the security of the components of the firewall for potential exposures by probing selected hosts to identify available services, moved or hidden services, and potential vulnerabilities with FTP options, sendmail, NFS, rexec, Telnet, rsh, denial-of-service attacks, IP spoofing options, and common accounts.

It should be noted that the Internet project is a relatively new initiative for Starcross and our review was performed while certain aspects of the project were still under development. Where appropriate, notations have been made to indicate those issues that IT management is aware of. By design, such issues as increased programmer access and lack of documentation have started to be addressed or will be addressed later in the project. As previously mentioned, senior Starcross management understands and accepts any increased internal control risks associated with the development methodology.

Methodology

1. Through inquiry and observation, assess policies and procedures related to Internet connectivity.
2. Through inquiry and observation, verify:
 - a. Existence of up-to-date standards for the maintenance of system security options and configurations

INFORMATION SECURITY ARCHITECTURE

- b. Procedures and controls for requesting security system software changes
 - c. Adequacy of testing and approval procedures performed before changes are moved into production
 - d. Extent of documentation present and the procedures for updating documentation for changes made to security system software
3. Through inquiry and observation, evaluate the procedures in place to monitor and log unauthorized activities. Determine if Starcross personnel are adequately reviewing these logs and following up on any deviations.
4. Through inquiry and observation, evaluate:
 - a. Procedures for defining and assigning classification levels to sensitive data
 - b. Implementation and impact of operating system and router security control features
 - c. Policies and procedures for granting access authority based on level of access needed, including remote access
 - d. Required approval and documentation of new, modified, or terminated user access authorities
 - e. Procedures for restricting users to selected data and programs
 - f. Procedures for automatic suspension of user IDs and terminals after a designated number of unsuccessful access attempts and the related reinitialization procedures
 - g. Policies and procedures to prevent the introduction of foreign programs and data that could contain viruses
 - h. Policies and procedures to ensure that only authorized execution of programs occur
5. Through inquiry, determine what types of criteria are being used for packet filtering (e.g., source IP address, destination IP address) and evaluate the appropriateness of this criteria.
6. Through observation, determine that there are physical security measures to prevent deliberate destruction or theft of equipment and software.
7. Through inquiry, evaluate the adequacy of backup and recovery procedures.
8. Through observation, verify the following physical environment characteristics:
 - a. Access-controlled areas
 - b. Roster of authorized persons
 - c. Environmental controls
 - d. Emergency contact information
9. Through observation and inquiry, verify that there are formalized procedures at Starcross to monitor new releases and findings on security.

Strengths

Internet User Guidelines. A detailed Internet Application Agreement has been developed and a customer's signature is required before they are given an account and access to the application via the Internet. This agreement includes a detailed description of the types of services offered, how to use the service, liabilities for unauthorized transactions, and how to resolve problems. Starcross personnel have developed a policy for Internet usage for employees having Internet access.

Detecting and Acting on Intrusion Attempts, Including an Incident Response Plan. As with any sensitive system or application, it is critical that log files are reviewed by a knowledgeable individual to ensure that intrusion attempts or security anomalies are discovered before any or significant damage has occurred. In addition, an incident response plan sets forth all of the procedures to follow in the event of an attack. For example, there should be a list of numbers and contacts to call when an incident is occurring or has been discovered.

Starcross has implemented and is in the process of refining and documenting this practice.

Router Security. The router configuration and access control lists have been reviewed and appear to be properly configured to minimize risk to the Internet application and Starcross, Inc. The configurations were effective during the Internet Security Scans and did not permit penetration through the routers to Starcross' internal network.

PC Manual. A PC Manual for the policies related to personal computing activities has been developed and defines the roles and responsibilities of committees, departments, and individuals throughout Starcross related to PC use and maintenance. This manual contains an Internet Security Policy and addresses the requirements for physical security, the use of access control software, backup and recovery, and the use of anti-virus software.

Physical Security. Computer equipment, software, programs, and information are stored in a locked computer room. In addition, the room is equipped with climate control features, fire suppression and detection features, and is adequately monitored. Access to the Liberty Commons site where the Data Processing Center is located requires both a card and keypad code to enter those areas.

External Scans. Starcross has contracted with an outside firm to conduct monthly external security scans using ISS software. These scans have been occurring since November 1999.

Report of Issues

The intent of this assessment was to document and evaluate the adequacy of established controls, identify weaknesses and related business risks, and provide recommendations to strengthen current controls. The following list of concerns relate to more than one component of the Internet and have been discussed with personnel who are responsible for the maintenance and administration of the component affected by the issue. Issues for a specific component are listed under the Report of Issues section for that component.

Programmer Access

It is the intention of Starcross' IT management to have consistent change control procedures across all processing platforms (i.e., mainframe, LAN, PC, UNIX). However, at the time of our review, the Internet project was still in the development phase. As a result, certain "standard" change control procedures, such as restricted programmer access to production files and documented sign-offs prior to programs being introduced into a production environment, were not consistently applied to all aspects of the project.

As defined by Starcross development methodologies, IT management stated that until the production environment became more stable and did not require so many changes, turnover and documentation were best handled by the programmers with the expertise on each system component. During the project, programmers did have more access than would typically be granted in accordance with host system standards. However, this increased access was deemed to be an acceptable level of risk by IT management.

It is understood by IT management that proper segregation of duties, appropriate documentation, and separate test and production environments are components of an effective change control program. IT management is also aware that without implementing a change control policy, changes could go into production unauthorized, untested, and unapproved. Starcross management is aware of these issues and assumes the increased internal control risk until the environment is more stable.

Suggested Action: As soon as possible, implement the appropriate change control procedures that are consistent with the control objectives found in Starcross' mainframe environment.

Action Taken:

Tools Usage

Starcross can take advantage of tools available for streamlining the process of monitoring, detection, and reporting. Without the proper use of technology to administer monitoring, detection, and reporting, incidents could go unnoticed.

Suggested Action: Starcross may want to consider the purchase of ISS SafeSuite so that the entire firewall, including routers and Web server, can be monitored. The following ISS tools can be installed and be run as part of the ongoing security monitoring of the systems:

- COPS (Computer Oracle and Password System)
 - System integrity checker tool
 - Bad permissions on critical files and directories
 - Malformed configuration files
- TIGER (Texas A&M University security assessment tools)
 - System integrity checker tool
 - Companion to COPS
 - Scans a UNIX system for security problems in a similar manner to COPS
- CRACK (password detection utility)
 - Scans the UNIX password file (/etc/passwd) for easy-to-guess passwords
- TRIPWIRE (directory and file checksum utilities)
 - Auditing
 - File integrity checker
 - Compares a designated set of files and directories against information stored in a previously generated database. Appended, added, or deleted files are flagged and reported. Tripwire is used to take a snapshot of the directory structure. Tripwire creates a signature of a file's time stamp, size, permission, and crc or other checksum data. It is extremely useful for detection of modified executable files (Trojan horses) and configuration files.
- TCP WRAPPERS (Network access control and logging system)
 - Allows monitoring and filtering of incoming requests for services started by inetd, such as Finger, Telnet, and FTP

Starcross has contracted with a outside firm to conduct monthly external security scans using ISS software. These scans have been occurring since November 1999.

ROUTERS

Methodology

1. Through review of the router access control lists, we confirmed our understanding of the router configurations (i.e., those services not specifically permitted are denied) and control settings.
2. Internet Security Scanner was used to probe the routers for known security vulnerabilities. The scan was performed both from the public Internet and internal Starcross network.

Strengths

Router Access Lists. After reviewing the router access control lists, the configurations appear to be sufficient to protect the firewall components and internal network.

Internet Security Scan. Internet Security Scanner was unable to identify any known security vulnerabilities existing in the current router configurations.

Password Encryption. Starcross has implemented a password-encryption option pertaining to the privileged mode command/configuration service. Accordingly, anyone performing a write terminal and show configuration command will not be able to determine the router's privilege mode password.

Session Timeouts. The timeout feature for unattended console sessions has been implemented. This option provides an additional security feature to disable a router console after a set period of time of inactivity. This helps to ensure that modifications cannot be made to router configurations if the console is accidentally left unattended.

Report of Issues

None noted.

PIX FIREWALL

Methodology

1. Through observation, we assessed the firewall configuration for denying and permitting services.
2. Internet Security Scanner was used to probe the firewall for known security vulnerabilities. The scan was performed both from the public Internet and internal Starcross network.

Strengths

Firewall Configuration. After reviewing the firewall configuration and results of the Internet Security Scanner, the configurations appear reasonable to protect the firewall components and internal network.

Report of Issues

Internet Security Scanner. The external (i.e., public Internet) security scan did not identify any security vulnerabilities associated with the Pix firewall, primarily due to the strong configuration of the exterior Cisco router. The internal scan revealed several low-risk vulnerabilities. These vulnerabilities should be reviewed with Unisys to determine if they are results of improper configuration or services that should not be enabled.

Unisys has defined appropriate configurations for these servers and the services identified may be required for proper operation of the interface. However, these services, if not properly monitored, could result in a security incident if exploited.

Suggested Action: Eliminate unused services and properly configure parameters that are not appropriate.

Action Taken:

UNIX SERVER

Methodology

1. Verify that secure authentication and encrypted access are being provided.
2. Interview administrator responsible for the configuration of Firewall-1. Interview administrator responsible for programming changes to the Internet application. Interview administrator responsible for UNIX.
3. Obtain an organizational chart and evaluate the extent of segregation of duties within Data Processing.
4. Verify that employee technical knowledge is adequate.
5. Obtain policies and procedures related to the firewall and evaluate the extent of administration and enforcement.
6. Evaluate the procedures followed when personnel are transferred or terminated. Obtain the site network security policy, topology diagram, and protocol list, and discuss each with the network administrator.
7. Review the diagram, policy, and narrative for consistency.
8. Secure connections. Through inquiry, gain an understanding of the secure connection mechanisms being used.
9. Test SSL mechanism through the Netscape browser to ensure that encryption is operating properly from the Starcross Web site.
10. Through inquiry, obtain support that site operators are aware of the purpose, origin, and integrity of all CGI programs in the site's "cgi-bin."
11. Perform a manual assessment of the UNIX operating system. We requested the following from the UNIX administrator:
 - a. /etc/passwd — user password file to verify which users have access to the system and who has root access
 - b. /etc/shadow — shows important log-on and password information
 - c. /etc/inetd.conf — shows what services are running or disabled
 - d. /etc/host.equiv — shows what hosts are on the system
 - e. /etc/group — shows the extent of the use of groups
 - f. /etc/default/login — shows the log-in parameters of the users and what shell they use
 - g. /etc/default/passwd — shows the default directory of each user

INFORMATION SECURITY ARCHITECTURE

- h. `/etc/syslog.conf` — shows information on system logs
 - i. `etc/default/su` — shows who is able to su to root
 - j. `/etc/ftpusers` — shows which users are granted ftp access
 - k. `/etc/services` — shows the services running on the system
 - l. `/var/adm/sulog` — shows the number of su attempts
12. Execute the following commands:
- a. User-defined Trusted hosts: `find / -name .rhosts -exec ls -al {} \; -exec cat {} \;`
 - b. SUID and GUID programs: `find / \ (-type f -perm -002000 -o -type f -perm -004000 \) -exec ls -al {} \; -print`
 - c. World Writable Directories: `find / -type d -perm -2 -exec ls -dl {} \; | grep -v .rsrc`
 - d. World Writable Directories Without Sticky Bit: `find / -type d -perm -0002 -a ! -perm -1000 -exec ls -dl {} \; | grep -v .rsrc`
 - e. World Writable Files: `find / -type f -perm -2 -exec ls -al {} \; | grep -v .rsrc`

Strengths

Firewall and Internet Security Scanner. After reviewing the firewall configuration and results of the Internet Security Scanner, the configurations appear reasonable to protect the firewall components and internal network. Firewall-1 is a solid platform that has proven in the industry to be a secure firewall if configured properly.

Employee Technical Ability. Employee technical knowledge is excellent and Starcross is providing training to increase existing knowledge.

SSL Encryption. SSL uses public-key encryption to exchange a session key between the client and server; this session key is used to encrypt the HTTP transaction (both request and response). Each transaction uses a different session key so that if someone manages to decrypt a transaction, that does not mean that they have found the server's secret key; if they want to decrypt another transaction, they will need to spend as much time and effort on the second transaction as they did on the first.

Report of Issues

Internet Security Scanner. Both the external and internal security scan identified two low-risk security vulnerabilities associated with the sendmail program. The sendmail program is the predominant software used in UNIX-based e-mail systems. The security scans identified that the verify (VRFY) and expand (EXPN) options have been enabled. The verify and expand options could provide valuable information to intruders attempting to gain unauthorized access to the network.

Suggested Action: We recommend disabling the sendmail verify and expand options by adding the lines “OPNOVERFY” and “OPNOEXPN” in the *sendmail.cf* configuration file.

Action Taken: Per IT management, this has been implemented since our review.

CGI Script Security Testing

CGI scripts are a major source of security holes. Although the protocol is not inherently insecure, CGI scripts must be written with just as much care as the server application itself. Unfortunately, some scripts fall short of this standard.

Although functional testing has been performed on the CGI scripts purchased from Edify, the testing procedures do not include tests for potential security vulnerabilities.

Suggested Action: Starcross should consider performing rigorous security testing of all purchased and developed CGI scripts to verify the integrity of the scripts and ensure they do not introduce unintentional security holes.

Firewall-1 Activity

The UNIX server is acting as a multipurpose Internet server. Currently, this server is responsible for not only hosting Starcross’ Internet home page, but is also acting as a proxy firewall and e-mail server.

After the external router, the UNIX server is Starcross’ primary defense against external threats and attacks. Any service or activity on the UNIX server could introduce unintentional software bugs or configuration errors that may lead to security holes or breaches.

Suggested Action: Consideration should be given to reconfigure the UNIX server to provide the smallest set of services possible. At a minimum, Web development should be moved to a separate host. Per IT management, this is a resource issue and once additional resources are obtained, this issue will be eliminated.

Action Taken:

Logging and Monitoring

Although logging and monitoring procedures are being performed, these procedures are not formalized or documented. Employees should have knowledge of how to log and monitor events and must be aware of what is expected.

INFORMATION SECURITY ARCHITECTURE

Suggested Action: Firewall-1 can be configured to specify logging and alerting for any communication attempt, whether the attempt is allowed or not. Log and alert formats and actions are open and can be configured by the user. For every event, the relevant information is displayed. Fields can be displayed or hidden. Reports can be generated by applying selection criteria to chosen fields, providing compound and comprehensive views.

Action Taken: Applications have been created to assist in the review of system logs.

Programmer Access

Programmers have knowledge of the root password. With access to the root account, there is virtually no way to control their activities. There is a risk that changes could be introduced into the production Web application without authorization, testing, or approval. There is also a risk that sensitive firewall and operating system configuration settings/parameters are modified.

Suggested Action: Starcross should consider that programmer profiles be removed and that all Web development be moved to a separate host.

Action Taken:

Password Sharing for Administrative Accounts

During our review, we noted that responsibilities for administrative functions, pertaining to the maintenance and configuration of the UNIX server, are shared among several individuals within Starcross. These individuals share a vendor-supplied account and password to perform administrative functions and tasks. The risk of sharing one account is lack of an audit trail and accountability.

Suggested Action: All users who have administrative responsibilities should be uniquely designated with separate accounts. The UNIX su command should then be used if access to the vendor administrative account is required. This command provides an audit trail, which can be reviewed periodically for unusual activity.

Action Taken:

Access Level Profiles

There are no profiles on the UNIX server that limit access based upon required job function, responsibility, or required service. For example, users are not properly excluded for FTP access, and those users that

require e-mail only are not restricted to only e-mail. Access forms should state what level of access each user should be given when the access is requested. If access is not properly assigned by classification levels, sensitive data could be compromised.

Suggested Action: Develop a policy, or incorporate procedures for assigning access levels into the security policy.

Action Taken:

Password Changing

During our review, we noted that several user accounts on the UNIX server are not changing their password on a regular basis. Password controls are the primary authentication mechanism on the UNIX server. If users are not changing their passwords, it provides an easier atmosphere to compromise the user accounts.

Suggested Action: Users should be required to change their passwords at least every 90 days.

Action Taken:

World Read and Write Files

Configuration files, Web page files, and system logs were identified as being world readable and writeable. Anyone with an account on the UNIX server can view, change, or delete logs, Web page files, configuration files, Informix database files, etc. While the majority of these files probably pose no security risk, some may contain sensitive information and should be secured.

Suggested Action: Files containing sensitive or historical information be appropriately secured.

Action Taken: Per IT management, this issue has since been addressed.

Backup Administration

Most of the knowledge of certain areas resides with one individual for each of the four IT areas (i.e., UNIX, teleprocessing, security, and support/programming). In the event that any one person is not available, there would not be anyone with sufficient knowledge to pick up the pieces in that area.

Suggested Action: A backup to the individuals responsible for important areas should be trained and shared the knowledge that the other possesses.

Action Taken:

CONCLUSION

The Line of Business Security Plan is designed to provide a current state assessment of the operating environment controls, risks, and vulnerabilities. The document is a working document that will be updated as changes are made to improve the controls over the environment and subsequently reduce vulnerabilities and risks.

Each control that is identified in the environment should be described in the LOB Security Plan. Those weaknesses that have not yet been addressed should be documented and prioritized for resources. As the weaknesses are addressed, documentation should be provided in the “Action Taken” section of the document issue. The document should be updated as controls are identified, strengths are defined, and as vulnerabilities and risks are mitigated.

GLOSSARY OF TERMS

- BCP** — Business Continuity Planning
- DNS** — Domain Naming System
- email or e-mail** — Electronic mail
- FTP** — File Transfer Protocol
- IS** — Information Systems (sometimes used for Information Services)
- ISP** — Internet Service Provider
- ISS** — Internet Security Scanner
- IT** — Information Technology
- LAN** — Local Area Network
- NFS** — Network File System
- NMS** — Network Management System
- TCP/IP** — Transaction Control Protocol/Internet Protocol
- VAN** — Value-Added Network
- WAN** — Wide Area Network

Appendix D

Intrusion Checklist

STARCROSS CSIRT

INTRUSION CHECKLIST

Please fill out all fields. If a field does not apply, enter N/A. E-mail this form to starcirt@starcross.net. If you are unable to e-mail this form, you may send it by fax to 412-555-5567.

If you suspect that your system may be compromised, take the following procedures and complete this form.

- DO
 - Disconnect the system from the network
 - Access the system as root and perform a complete system backup to tape or CD
 - Confirm the integrity of the system backup and place in a restricted access location
 - Restrict physical access to the system until CSIRT can be contacted
 - Complete the following in detail and notify the Regional CSIRT
 - Disable associated user accounts, if known, until law enforcement determines investigative status
 - Enter N/A in the fields that do not apply
- DON'T
 - Turn the system off or reboot the computer
 - Finger or attempt to contact the source directly
 - Alter or change the system files on the suspicious system
 - Connect to the system over the network
 - Allow any suspected individuals access to the system

POC Name:

LAST:

FIRST:

Phone Number:

Position:

E-mail Address:

INFORMATION SECURITY ARCHITECTURE

System Administrator

Last Name:

First Name:

Years of Experience:

Formally Trained:

Yes

No

Phone Number:

E-mail Address:

Division or Department:

Department Manager Name:

LAST:

FIRST:

Phone Number:

Location Address:

Physical Location of System:

Only investigate the configuration of the system once a complete backup has been accomplished.

Target Information

Security Classification: Unclassified

IP Address of the Targeted System(s):

IP:

PORT:

Static

Dynamic

Serial Number of System:

Operating System of the Targeted System:

Version:

MAC Address of System NIC:

Fully Qualified Domain Name of the Targeted System
(i.e., `worstal.starcross.net`):

How long has the system been online?

Date or level of the latest patch (dd-*MMM*-*yyyy*):

System Hardware (i.e., Sun/Compaq/Dell):

Is system a Web server?	Yes	No
-------------------------	-----	----

Publicly accessible?	Yes	No
----------------------	-----	----

Is system a network server?	Yes	No
-----------------------------	-----	----

How many clients on the network?

How many servers on the network?

Security Mode of Operation (Dedicated/System, High/Multi-level, etc.):

Other software installed on the system:	Yes	No
---	-----	----

 If yes, what type (IRC, Napster, etc.)?

What AV product is installed on the system?

Norton McAfee None Other

What was the latest AV update?

INFORMATION SECURITY ARCHITECTURE

Were there any alerts from the AV product? Yes No

If yes, identify the alert/warning:

Accreditation Date (dd-MMM-yyyy):

Trusted Host: (What systems trust this host?)

IP Address:	IP Address:
IP Address:	IP Address:
IP Address:	IP Address:
IP Address:	IP Address:

Is there an approved log-in banner? Yes No

Information contained on the system:

Information available on the network:

What was the system used for: (admin, finance, logistics, etc.)?

Is there an Intrusion Detection Sensor (IDS) monitoring this network? Yes No

If yes, what type? (Real Secure/Shadow/NID/JID/snort/etc.)

Are IDS logs available? Yes No

Can they be provided / accessed? Yes No

Is there a firewall protecting this system? Yes No

If yes, what type? (Sidewinder / Gauntlet / Raptor / etc.)

Are firewall logs available? Yes No

Can they be provided / accessed? Yes No

When was detected (dd-MMM-yyyy):

Who discovered the intrusion?

LAST:

FIRST:

How was the intrusion detected? What suspicious activity preceded / caused the investigation?

What actions did the system administrator/security specialist take in this incident to date?

Has the site been blocked at the controllable security routers?

Yes

No

If yes, how?

How was the intruder able to access the system?

What was the exploit used, if identified?

Level of access gained by the intruder? (root/user level):

Was the system used to target another site?

Yes

No

IP Address:

IP Address:

IP Address:

Security Status: Offline?

Yes

No

If no, why is the system still online? (PDC/BDC/Exchange Server/etc.)

INFORMATION SECURITY ARCHITECTURE

Has the system had a vulnerability assessment conducted in the past? Yes No

If yes, when? (dd-MMM-yyyy)

How?

By Whom?

Agency:

LAST:

FIRST:

Has the system been compromised previously? Yes No

If yes, when? (dd-MMM-yyyy : hh:mm:ss):

Has the system administrator changed root password for other systems? Yes No

If yes, when: (dd-MMM-yyyy):

Were files uploaded to the target system? Yes No

If yes, what type?

Names of files identified:

Can the files be provided? Yes No

Were files downloaded by the target system? Yes No

If yes, what type?

Names of files identified:

Was the system scanned after the backup was conducted? Yes No

If yes, when (dd-MMM-yyyy)?

By whom?

Agency?

LAST:

FIRST:

Can the results be provided? Yes No

Countermeasure installed on the system? (i.e., TCP wrapper, shadow password files/etc):

IMPACT: (i.e., compromised/denial of service/altered data/loss of service/ etc.)

Manhours / people involved (investigation):

Manhours / people involved (recovery):

Manhours / people involved (lost productivity):

Any suspicious e-mails sent from the user's account? Yes No

If yes, what was the destination address (include copy)?

Source Information

IP Address identified as potential sources (from files or logs):

IP:

PORT:

Source Country:

INFORMATION SECURITY ARCHITECTURE

Fully qualified domain name if available or resolved:

Suspected persons attempting to gain access, if known:

LAST: FIRST:

LAST: FIRST:

LAST: FIRST:

Date / Time of the Session:

START (dd-**MMM**-yyyy, mm:ss:hh):

STOP (dd-**MMM**-yyyy, mm:ss:hh):

Attack Method:

Type of Protocol: TCP UDP ICMP Other

Did a commercial entity provide notification to the POC? Yes No
(send comments)

Did a commercial entity provide logs or files to the POC? Yes No
(send comments)

Your e-mail address:

Index

A

Access control(s)

- application controls assessments, 169
- awareness and training program, 155–156
- banking industry incident, 3–6
- baselines and risk assessments, 103, 112–113
- change management, 117
- contractors and third-party vendors, 194, 195–196
- enterprise management tools, 175
- evaluation and certification of systems, 127
- incident/emergency response, 216–217
- integrity of system, 1
- layered, 9
- line of business (LOB) security plan, 362–363
- network and application administrator responsibilities, 37
- network security assessment workplan, 312–313
- organization/infrastructure, 26–27
- security coordinator or liaison responsibilities, 35, 36
- security officer responsibilities, 32
- software, 170
- source libraries, 116
- strategic information technology (IT) plan questions, 22
- types of controls, 15–16
- types of threats, 11–12
- Windows NT, 129
- Windows NT assessment workplan, 323–324

Access control lists (ACLs), 112, 113, 130

Accessibility, availability of information, 2

Access points

- control placement, 170–171
- network, 9–11

Access privileges and policy

- administrative controls, 134
- policy manual sample
 - authorization, 245–246
 - implementation, 252–254

Accountability, policy manual sample, 245

Accounting systems, chief financial officer responsibilities, 31

Account integrity, enterprise management tools, 174

Accounts payable, separation (or segregation) of duties, 113, 114

Accounts receivable, separation (or segregation) of duties, 114

Accuracy, application control objectives, 169

ACERT (Army Computer Emergency Response Team), 201, 206, 208, 215

ACF2, 113

Acknowledgement form, information security policy, 259–261

Administration, security, 45

- baselines and risk assessments, 102
- telecommunications security assessment, 328–329

Administrative controls, 15, 16, 17

- baselines and risk assessments, 133–134
- change management, 117
- organization/infrastructure, 37, 46

Administrators

- awareness and training program, 146, 151–152
- compliance/control implementation, 166–167, 177
- organization/infrastructure, 37, 46, 47
- policies, standards and procedures, 99

Advisories, 32, 225

AIS (Automated Information System), 201

Alerts and warnings, 32, 225

- awareness and training program, 156
- incident/emergency response, 205–206
- professional organizations, 159–160

ALERT team, emergency response plan, 332–333

Analysis

- business impact, 104, 109
- incident/emergency response
 - artifact handling, 207–208
 - incident, 216–218
 - incident handling, 206
 - methodology, 208
- mergers and acquisitions, 183–186

Announcement letter sample, 57–58

INFORMATION SECURITY ARCHITECTURE

- Announcements, security, 225
- ANSIR (Awareness of National Security Issues and Response), 156
- Anti-virus procedures, *see* Viruses/anti-virus procedures
- Application administrators
 - compliance/control implementation, 166–167
 - organization/infrastructure, 37, 46
- Application coordinators,
 - organization/infrastructure components, 28
- Application owners, *see* Owners/ownership
- Applications/application controls
 - audits, 169–170
 - network security assessment workplan, 315–316
 - organization/infrastructure, 37, 46
 - responsibilities
 - chief information officer, 29
 - security officer, 32
 - risk assessment, 103, 111–136
 - access controls, 112–113
 - audit trails, 114
 - authentication, 114–116
 - change management, 117
 - current and future Internet connections, 122–123
 - database security, 117–119
 - development and implementation, 103, 116–117
 - electronic mail and virtual office, 123–124
 - emergency response, 120–121
 - networks, 119–120
 - networks, gateways separating corporate WAN and lines of business, 122
 - networks, placement of WAN resources at client sites, 124–125
 - operating system security assessment, 125
 - remote access, 121
 - separation (or segregation) of duties, 113–114
 - Windows NT, 125–132
- Application security assessment, 301–307
 - authentication, 303–304
 - authorization, 302–303
 - computer operations, application-specific, 306
 - database, 306–307
 - development and implementation, 305–306
 - integrity, 304–305
- Applications programmers, change management, 117
- Application system utilities, audit trails, 114
- Appropriate operation, application owner and, 4–5
- Architecture
 - chief information officer responsibilities, 30
 - client/server environments, 6–11
 - controls overview, 11–17
 - controls, 14–17
 - incident, 12–14
 - risk, 12–14
 - threat, 11–12
 - implementation, 240–241
 - initiation of ISA, project management, 56–71
 - questions to evaluate security, 22–23
 - reasons for, 2–6
 - security team responsibilities, 34
 - strategic information technology (IT) plan, 17–22, 52
 - description of organization, 18
 - integrated framework, 20, 21
 - overview/executive summary, 18
 - relationship to organization's strategic business plan, 19
 - scope, viability, and modification of plan, 18–19
 - strategic goals for information technology, 19
- Area networks, 18, 50; *see also* Networks/LANs/WANs
- Army Computer Emergency Response Team, *see* ACERT (Army Computer Emergency Response Team)
- Artifact handling, incident/emergency response, 207–208
- Assessments
 - application security, 301–307
 - baselines and risk assessments
 - organization of security function, 103
 - policies, standards and procedures, 104
 - risk-related programs, 104–105
 - security plan, 104
 - merger/acquisition impact analysis, 185
 - organization/infrastructure, management and assessment tools, 37–38
 - policies, standards and procedures, 80–81

- strategic information technology (IT)
 - plan, 20
- Assessment workplan, operations, 287–299
 - computer operations, 296–299
 - backup and recovery planning, 297–298
 - physical and environmental security, 296–297
 - problem management, 299
 - systems management, 297
 - operating environment, security
 - administration and management, 287–293
 - information security plan, 290–291
 - operating environment, 287–289
 - policies, standards and procedures, 291–292
 - risk assessment, 292–293
 - security organization, 289–290
 - operational security programs, 293–296
 - compliance with legal and regulatory requirements, 295–296
 - microcomputer security, 294–295
 - security monitoring, 293–294
 - virus controls, 294
- Assessment workplans
 - network security, 309–319
 - access controls, 312–313
 - backup and recovery, 316
 - external access, 316
 - hardware/software/circuits, 315–316
 - Internet, 316–317
 - management, 311–312
 - operating environment, 309–311
 - remote access, 314–315
 - third-party providers, 314
 - telecommunications, 327–330
 - Windows NT, 321–325
- Assets
 - baselines and risk assessments, 102
 - merger/acquisition impact analysis, 185
 - policy manual sample, 245
- Audit function, compliance, 167–172
- Audits
 - compliance/control implementation, 165
 - compliance testing, 177
 - contractors and third-party vendors, 195–196
 - enterprise management tools, 174
 - ISA project deliverables, 71, 74
 - logs, 195–196
 - organization/infrastructure
 - compliance, 42
 - component, 42
 - external, 41–42
 - internal, 39–41
 - responsibilities, policy manual sample, 250–251
- Audit trails
 - baselines and risk assessments, 114
 - Windows NT, 131
- Authentication, user, 131
 - application security assessment, 303–304
 - baselines and risk assessments, 114–116
 - contractors and third-party vendors, 194
 - integrity of system, 1
 - policy objectives, 247
 - secure tokens, 115
 - security officer responsibilities, 32
- Authorization
 - application security assessment, 302–303
 - policy manual sample, 245–246
- Automated Information System (AIS), 201
- Automated tools
 - access controls, 170
 - assessment, line of business (LOB)
 - security plan, 345
 - enterprise security management, 173–176
- Automatic attendants, 132
- Availability, information, 2, 247
- Awareness and training program, 139–163
 - architecture, 75
 - chief information officer responsibilities, 30
 - development of, 161–162, 163
 - ISA project deliverables, 71
 - objectives, 139–147
 - level of security awareness among existing employees remains high, 146–147
 - recognition and notification of potential violations, 142–146
 - responsibility for protecting enterprise's information assets, 139–140
 - understanding value of information security, 140–142
- ownership of information and resources, 49
- policy manual sample, 254–255
- program considerations, 147–160
 - benefits are difficult to measure in short term, 148–149
 - effectiveness is based on long-term commitment of resources and funding, 147–148
 - scoping target audience, 149–154

INFORMATION SECURITY ARCHITECTURE

- security organizations, 159–160
- target audience, reaching, 154–159
- security coordinator or liaison
 - responsibilities, 36
- security officer responsibilities, 32
- Awareness of National Security Issues and Response (ANSIR), 156

B

- Backup power, 108
- Backup and recovery
 - application development and implementation, 117
 - assessment workplan, 297–298
 - baselines and risk assessments, 103, 109–110
 - controls, 169
 - enterprise management tools, 174
 - microcomputer security, 107
 - network security assessment workplan, 316
- Backups, e-mail, 86
- Balance controls, application development and implementation, 116
- Banking industry
 - firewall selection incident, 3–6
 - risk assessment, 182
 - security organizations and working groups, 94
- Baselines and risk assessments, 101–137
 - application controls assessments, 111–112
 - access controls, 112–113
 - application development and implementation, 116–117
 - audit trails, 114
 - authentication, 114–116
 - change management, 117
 - current and future Internet connections, 122–123
 - database security, 117–119
 - electronic mail and virtual office, 123–124
 - emergency response, 120–121
 - gateways separating corporate WAN and lines of business, 122
 - network assessments, 119–120
 - operating system security
 - assessment, 125
 - placement of WAN resources at client sites, 124–125
 - remote access, 121
 - separation (or segregation) of duties, 113–114
 - windows NT, 125–132
 - application security, 301–307
 - architecture, 75
 - assessment workplan, 287–299; *see also* Assessment workplans
 - components of internal control, 167
 - computer operations (section III), 108
 - backup and recovery, 109–110
 - computer systems management, 110
 - physical and environmental security, 108–109
 - problem management, 110–111
 - definitions, 101–102
 - high-level security assessment (section I), 103–105
 - organization of security function, 103
 - policies, standards, 104
 - risk-related programs, 104–105
 - security plan, 104
 - ISA project deliverables, 71
 - merger/acquisition impact analysis, 185
 - policies, standards and procedures, 80–81
 - responsibilities for, 35
 - security assessment phased approach, 102–103
 - security life cycle, 176
 - security operations (section II), 105–107
 - compliance with legal and regulatory requirements, 108
 - computer virus controls, 106
 - microcomputer security, 107
 - security monitoring, 105–106
 - strategic information technology (IT) plan, 20, 52
 - telecommunications assessments, 132–136
 - workplans, assessment
 - application security, 301–307
 - general security, 287–299; *see also* Assessment workplans
 - network security, 309–319
 - Windows NT, 321–325
- Baselining, security system, 5
- Batch controls, 116, 168
- Benefits, awareness and training program, 148–149
- Binder labels, ISA project management, 66
- Boards of directors, understanding risk, 181
- Bridges, 8
- Brochures, 158–159
- Budget, *see* Funding/budget

- Business continuity plan, strategic information technology (IT) plan, 20
 - Business impact analysis (BIA), 104, 109
 - Business objectives, *see also* Strategic Business Plan
 - chief financial officer responsibilities, 31
 - security architecture, 20
 - security life cycle, 176
 - strategic information technology (IT) plan and, 50–51
 - strategic information technology (IT) plan questions, 23
 - Business plan, strategic information technology (IT) plan and, 50–51
 - Business process reengineering, 18
 - Business security coordinator, 45
 - Business units
 - independent operations throughout, 186–188
 - security program pitfalls, 183–186
- C**
- Call center, incident/emergency response, 208
 - Call detail record (CDR), 133
 - Calling cards, 132
 - Central exchanges (Centrex), 132
 - Centralized computing,
 - organization/infrastructure, 26
 - CERT® (Computer Emergency Response Team), 88, 202, 203
 - advisories, security officer responsibilities, 32
 - awareness and training program, 156
 - management and assessment tools, 37–38
 - United States (US-CERT), 221
 - CERT (Computer Emergency Response Team)/CC, 208, 214, 218, 219, 220
 - constituency definition, 227
 - incident/emergency response, 203
 - Certification of systems, 126–128
 - Chain of custody, 216–217
 - Change management, 241
 - awareness and training program, 150, 151
 - baselines and risk assessments, 103, 117
 - controls, 168
 - line of business (LOB) security plan, 346
 - Charter
 - ISA project deliverables, 71–72
 - ISA project management, 58–62
 - sample, 56
 - Checklist, intrusion, 365–372
 - Chief financial officer
 - information security architecture project, 56
 - organization/infrastructure components, 28, 31–32
 - understanding risk, 181
 - Chief information officer
 - information security architecture project, 56
 - organization/infrastructure components, 28, 29–31
 - CICS, access controls, 113
 - Cipher locks, 108
 - CIRC (Computer Incident Response Center), 220
 - Circuits, network security assessment
 - workplan, 315–316
 - CIRT (Computer Incident Response Team), 201
 - Classification
 - information, 140
 - resources, 147
 - Classification methodology
 - baselines and risk assessments, 104
 - ISA project deliverables, 72
 - strategic information technology (IT) plan, 20
 - Class of restriction (COR), calling privileges, 133
 - Class of service (COS), calling privileges, 133
 - Client-server environments, 50
 - access paths, 170–171
 - anti-virus update procedure, 283–284
 - architecture, 6–11
 - strategic information technology (IT) plan, 18
 - Client sites, WAN placement, 124–125
 - Closed processing environments, defined, 7
 - Codes of conduct and ethics, 146
 - Collaborative computing, 18, 50
 - Committee
 - executive, *see* Executive committee for security
 - security advisory, 35
 - strategic information technology (IT) plan questions, 22
 - Communication mechanism
 - awareness and training program, 162
 - components of internal control, 167
 - policies, standards and procedures as, 79
 - risk assessment results, 181
 - Communications Fraud Control Association (CFCA), 160

INFORMATION SECURITY ARCHITECTURE

- Communications networks/technologies, *see also* Telecommunications
 - architecture, 9–10, 18
 - merger/acquisition impact analysis, 185
 - organization/infrastructure, 50
- Completeness, application control
 - objectives, 169
- Complex instruction set computer (CISC),
 - Windows NT, 125–126
- Compliance, 6, 165–177
 - architecture, 75
 - assessment workplan, 295–296
 - baselines and risk assessments, 103, 108
 - enterprise management tools, 173–176
 - ISA project deliverables, 71
 - legal and regulatory requirements, 108
 - levels of
 - audit function, 167–172
 - component owner, 166–167
 - security team, 172–173
 - line of business (LOB) security plan, 173
 - merger/acquisition impact analysis, 185
 - organization/infrastructure, 42
 - strategic information technology (IT) plan, 20, 52
- Component audits,
 - organization/infrastructure, 42
- Component owner, *see* Owner, component
- Computer Emergency Response Team, *see* CERT (Computer Emergency Response Team)/CC
- Computer Incident Advisory Center (CIAC), 219, 220
- Computer Incident Response Center (CIRC), 220
- Computer Incident Response Team (CIRT), 201
- Computer operations
 - application security assessment, 306
 - assessment workplan, 296–299
 - backup and recovery planning, 297–298
 - physical and environmental security, 296–297
 - problem management, 299
 - systems management, 297
- baselines and risk assessments (section III), 108
 - backup and recovery, 109–110
 - computer systems management, 110
 - physical and environmental security, 108–109
 - problem management, 110–111
- Computer Security Incident Response Team, *see* CSIRT (Computer Security Incident Response Team)
- Computer Security Institute (CSI), 160
- Computer systems management, baselines and risk assessments, 110
- Computing policy, network management, 263–265
- Confidentiality
 - awareness and training program, 150
 - defined, 1
 - e-mail policy, 86
 - employee responsibility for, 3
 - human resources, responsibilities of, 37
 - line of business (LOB) security plan, 350–351
 - password, 42
 - security coordinator or liaison responsibilities, 36
- Confidentiality agreements
 - contractors and third-party vendors, 194
 - temporary employees and consultants', 143–144
- Constituency definition, 227
- Consultants, corporate espionage risk, 143–144
- Contact person
 - awareness and training program, 142–143
 - emergency response plan, 334
 - incident/emergency reporting, 210
 - problem management, 111
- Containment, incident/emergency response, 208, 209, 215, 221–223
- Contests, 156–157
- Contingency planning, microcomputer security, 107
- Continuity, security team responsibilities, 34
- Continuous network monitoring, 197
- Contractors, *see also* Third-party vendors and service providers
 - administrative controls, 133–135
 - network management, 192–196
 - security procedures, 162
- Control-Alt-Delete (secure attention sequence), 130
- Control criteria, external audit, 41
- Control environment, components of
 - internal control, 167
- Controls
 - architecture overview, 11–17
 - controls, 14–17
 - incident, 12–14
 - risks, 12–14
 - threat, 11–12

- baselines and risk assessments, 102
 - compliance, audit function, 167–172
 - contractors and third-party vendors, 195
 - network and application administrator responsibilities, 37
 - policy manual sample, 251, 255–257
 - policy objectives, 246–247
 - security life cycle, 176–177
 - security officer responsibilities, 32
 - security team responsibilities, 34, 35
 - Coordination, incident/emergency response, 209, 219–221
 - Coordinators, security, *see* Security coordinators or liaisons
 - Copyrights and license compliance, 107, 252
 - Corporate espionage, 143–146
 - Corporate policies, policy manual sample, 256
 - Costs, pitfalls of effective ISA program, 197, 198
 - Crossword puzzle, 157–158, 163
 - CSIRT (Computer Security Incident Response Team), 201, 202
 - development of, 226–229
 - eradication, 223
 - goals and responsibilities, 203–205
 - incident/emergency response, 202
 - coordination of response, 219
 - incident handling methodology, 208
 - notification, 224–225
 - recovery, 224
 - reevaluation of, 236
 - issues in development of, 230–236
 - funding, 230–231
 - legal issues, 234–235
 - management buy-in, 231
 - policy development, 233–234
 - reevaluation of CSIRT operations, 236
 - staffing and training, 231–232
 - policy manual sample, 255
 - triage, 214–215
 - types of announcements, 225–226
 - Culture, corporate, 198
 - Custodian level responsibility, 45, 47
 - Customer satisfaction, 30
- D**
- Databases
 - application security assessment, 306–307
 - baselines and risk assessments, 117–119
 - client-server environments, 8
 - Data integrity
 - application security assessment, 304–305
 - microcomputer security, 107
 - Data security officer, 26, 32
 - Data sharing, client-server environments, 8
 - Decentralization of processing, and security requirements, 2–3
 - Delegation of duties, and defining ownership, 46
 - Denial-of-Service (DoS) attacks, 213
 - Departmental management
 - access privilege requests, 253
 - awareness and training program, 146–147
 - organization/infrastructure components, 28, 36–37
 - responsibilities, policy manual sample, 250
 - Departmental policy, policy manual sample, 256
 - Detection, *see* Monitoring and detection
 - Detective controls, 16–17
 - Development and implementation,
 - applications
 - risk assessment, 103, 116–117
 - security assessment, 305–306
 - Dial-in service, 9, 121
 - Dial-out service, 9
 - Digital signature, 15–16
 - Direct Inward System Access (DISA), 135–136
 - Disaster recovery/business continuity plan
 - architecture, 75
 - baselines and risk assessments, 104
 - contractors and third-party vendors, 195
 - ISA project deliverables, 71
 - operating environment component identification, 47
 - policy manual sample, 255
 - strategic information technology (IT) plan, 20, 52
 - Windows NT assessment workplan, 322–323
 - Discretionary access control list (DACL), 129
 - Distributed computing
 - organization/infrastructure, 26
 - security officer responsibilities, 32
 - and security requirements, 2–3
 - Documentation, 43
 - administrative controls, 134
 - baselines and risk assessments, 102
 - chain of custody, 216
 - merger/acquisition impact analysis, 185
 - microcomputer security, 107

INFORMATION SECURITY ARCHITECTURE

- operating environment component
 - identification, 47
- ownership of information and resources, 48
- Document checklist, baselines and risk assessments, 104–105
- Dumpster diving, 144
- Duties, segregation of, 113–114

E

- Electronic commerce, 18, 50
 - Electronic data interchange (EDI), 9, 18, 48, 50
 - Electronic funds transfer (EFT), 9
 - E-mail, 9, 18, 50
 - anti-virus update procedure, 284
 - baselines and risk assessments, 123–124
 - computing policy, 264
 - incident/emergency response, 208
 - line of business (LOB) security plan, 351
 - merger/acquisition impact analysis, 185
 - organization/infrastructure, 26
 - policies, standards and procedures, 77, 83–87
 - security awareness training, 5–6
 - security policy, 267–269
 - Emergency maintenance, application development and implementation, 117
 - Emergency response
 - awareness and training program, 161
 - baselines and risk assessments, 120–121
 - contractors and third-party vendors, 195
 - ISA project deliverables, 71
 - Emergency Response Service, IBM, 156
 - Employees, *see also* Human resources;
Personnel
 - awareness and training program
 - responsibility and reporting requirements, 142–143
 - responsibility for security, 139–240
 - understanding value of information security, 140–142
 - human resources, responsibilities of, 37
 - information security policy
 - acknowledgment form, 259–261
 - policies, standards and procedures, 99
 - responsibilities, policy manual sample, 251
 - responsibility for security, 3
 - security awareness training, *see*
Awareness and training program
 - security coordinator or liaison
 - responsibilities, 35, 36
 - security program pitfalls, mainframe versus distributed computing cultures, 188–189
 - separation (or segregation) of duties, 113–114
 - strategic information technology (IT) plan questions, 22, 23
 - temporary employees and consultants' corporate espionage, 143–144
 - security procedures, 162
 - third-party vendors, 192–193
- Encryption, 87
 - Enforcement
 - Internet policy, 273
 - policy manual sample, 254
 - Engineering, information security, 44–45
 - Enterprise initiatives, chief information officer responsibilities, 29
 - Enterprise security management tools, 173–176
 - Environmental security, *see* Physical and environmental security
 - Eradication, incident/emergency response, 209, 215, 223–224
 - Espionage, corporate, 143–146
 - Evaluated products list (EPL), Windows NT, 126
 - Evaluation of systems, 127–128
 - Event, incident/emergency response, 00
 - Evidence collection, incident/emergency response, 209, 216
 - Executive committee for security
 - centralized versus decentralized security administration, 43
 - information security architecture project, 56
 - organization/infrastructure components, 28, 29, 30
 - responsibilities, policy manual sample, 249
 - security team supervision, 34
 - Executive-level responsibilities, pitfalls of effective ISA program, 180–181
 - Executive management
 - awareness and training program, 146, 151, 161
 - information security architecture project, 56
 - pitfalls of effective ISA program
 - lack of support, 180–181
 - lack of understanding of realistic risk, 181–182

- policies, standards and procedures, 79, 98
 - security officer and, 32, 33
- Executive summary, line of business (LOB) security plan, 338–340
- Expert systems, 18, 50
- External account managers, 195
- External audit
 - compliance testing, 177
 - organization/infrastructure, 41–42

F

- Facility restriction levels (FRLs), calling privileges, 133
- Federal Computer Incident Response Center (FedCIRC), 220
- File access, enterprise management tools, 174
- File allocation tables (FAT), 130
- File attribute changes, enterprise management tools, 174
- File transfers, Internet policy, 87
- Financial audit, 169
- Finger, 222
- Firewalls, 88
 - anti-virus update procedure, 284
 - banking industry incident, 3–6
 - incident/emergency response, 223–224
 - line of business (LOB) security plan, 358–359
 - merger/acquisition impact analysis, 185
 - organization/infrastructure, 26
- FIRST (Forum of Incident Response and Recovery Teams), 208, 220–221
- Flyers, 158–159
- Footprinting, 213
- Forensics, 00, 208, 209, 217
- Forum of Incident Response and Recovery Teams (FIRST), 208, 220–221
- For your information announcements, 225
- Funding/budget
 - awareness and training program, 147–148, 162
 - incident/emergency response, 230–231
 - organization/infrastructure, 26
 - pitfalls of effective ISA program, 197

G

- Gateways separating corporate WAN and lines of business, baselines and risk assessments, 122

- Goals/objectives IT security
 - security life cycle, 176
 - strategic information technology (IT) plan, 51, 52
 - strategic information technology (IT) plan questions, 23
- Graphical user interfaces (GUI), 7
- Group security ID, 129
- Groupware, 18, 50
- Guideline announcements, 225, 226
- Guidelines, departmental, 256

H

- Hardware/software/circuits, network security assessment workplan, 315–316
- Heads up announcements, 225
- Healthcare industry, 45
 - risk assessment, 182
 - security organizations and working groups, 94
- Help desk
 - administrative controls, 135
 - incident/emergency response, 208
 - organization/infrastructure components, 28, 39
 - problem management, 111
 - responsibilities, policy manual sample, 249–250
- High-level security assessment, 103–105
 - organization of security function, 103
 - policies, standards, 104
 - risk-related programs, 104–105
 - security plan, 104
- Hoaxes, 213
- Hot fixes, 131
- Human resources
 - access controls, 253
 - evolution of role, 35
 - organization/infrastructure components, 28, 37
 - ownership of information and resources, 48
 - pitfalls of effective ISA program, 198
 - responsibilities, policy manual sample, 250

I

- Identification, incident/emergency response, 215–216

INFORMATION SECURITY ARCHITECTURE

- analysis, 216
- methodology, 209
- Identification of users, 1, 131
- Image processing, 18, 50
- Impact analysis, mergers and acquisitions, 183–186
- Implementation of security initiatives
 - chief information officer responsibilities, 30
 - policy manual sample, 251–255
 - security life cycle, 176
- Incident
 - architecture
 - controls overview, 12–14
 - reasons for, 3
 - awareness and training program
 - employee recognition of potential violations, 142–143
 - scoping target audience, 151–154
 - incident/emergency response
 - analysis, 216–218
 - classification, 213
- Incident/emergency response, 201–238
 - architecture, 75
 - awareness and training program, 161
 - baselines and risk assessments, 104
 - Cert®/CC, 203
 - containment, 221–223
 - contractors and third-party vendors, 195
 - CSIRT
 - development of, 226–229
 - goals and responsibilities, 203–205
 - CSIRT, issues in development of, 230–236
 - funding, 230–231
 - legal issues, 234–235
 - management buy-in, 231
 - policy development, 233–234
 - reevaluation of CSIRT operations, 236
 - staffing and training, 231–232
 - eradication, 223–224
 - identification, 215–216
 - incident analysis, 216–218
 - incident classification, 213
 - incident response, 218–219
 - incident response coordination, 219–221
 - incident response handling methodology, 208–209
 - introduction, 201
 - intrusion checklist, 365–372
 - key organizations, 220–221
 - learning objectives, 201–203
 - notification, 224–226
 - reactive services, 205–208
 - alerts and warnings, 205–206
 - artifact handling, 207–208
 - incident handling, 206–207
 - vulnerability handling, 207
 - recovery, 224
 - reporting, 209–213
 - sample plan, 331–336
 - triage, 213–215
- Incident Response Handling (IRH), 201, 202, 208–209
- Industry-based knowledge, strategic information technology (IT) plan questions, 22–23
- Information, components of internal control, 167
- Information classification, baselines and risk assessments, 102
- Information resources
 - implementation, 251–252
 - ownership of, 45–49
- Information security engineering, 44–45
- Information security officer, professional organizations, 159–160
- Information security plan, assessment workplan, 290–291
- Information security policy
 - policies, standards and procedures, 81–82
 - sample, 243–257
- Information security policy acknowledgment form, 82, 259–261
- Information Systems Security Association, 160
- Infrastructure, security, *see* Organization/infrastructure, security
- Inheritance, 131
- Institute of Internal Auditors, 160
- Integrated IS architecture, 3
- Integrity, application security assessment, 304–305
- Integrity of information system
 - awareness and training program, 150
 - defined, 1–2
 - enterprise management tools, 174
 - policy objectives, 247
- Intelligent agents, 18, 50
- Inter-incident analysis, 218
- Intermediate distribution facilities (IDFs), 135
- Internal audit
 - compliance/control implementation, 171–172
 - compliance testing, 177

- organization/infrastructure, 39–41
 - responsibilities, policy manual sample, 250–251
 - Internal controls, chief financial officer responsibilities, 31
 - International Computer Security Association (ICSA), 160
 - Internet, access/security/policy, 9, 271–273
 - architecture, access points, 11
 - banking industry incident, 3–6
 - baselines and risk assessments, 122–123
 - corporate espionage, 144
 - line of business (LOB) security plan, 339, 353–357
 - merger/acquisition impact analysis, 185
 - network security assessment workplan, 316–317
 - organization/infrastructure, 26
 - policies, standards and procedures, 77, 82, 87–89
 - process for change, 90
 - security organizations and working groups, 95
 - strategic information technology (IT) plan questions, 22
 - Internet Engineering Steering Group (IESG), 88
 - Internet Engineering Task Force (IETF), 88
 - Internet resources
 - policies, standards and procedures information, 95
 - security lists, 275–276
 - Internet service providers (ISPs)
 - architecture, 11
 - incident/emergency response, 217
 - Internetworks, client-server environments, 8–9
 - Interview schedule, ISA project management, 67
 - Interview template, ISA project management, 68
 - Intra-incident analysis, 218
 - Introduction, incident/emergency response, 201
 - Intrusion, incident/emergency response, 213
 - Intrusion checklist, 365–372
 - Intrusion detection, *see also* Monitoring and detection
 - checklist, 365–372
 - contractors and third-party vendors, 195
 - incident/emergency response, 206
 - Inventory of assets
 - baselines and risk assessments, 102
 - merger/acquisition impact analysis, 185
 - Investment decisions, chief information officer responsibilities, 30
 - IRH (Incident Response Handling), 201, 202, 208–209
 - Issues discussion document, ISA project deliverables, 71, 72, 73
- J**
- Job description, security responsibilities, 140
 - Job function, access controls, 112
 - Job scheduling, controls, 168
- K**
- Kernel mode, Windows NT, 128
 - Key control, incident/emergency response, 216–217
 - Key organizations, incident/emergency response, 220–221
 - Keypad locks, 108
 - Keystroke recording software, 150
 - Key systems, 132
 - Keywords, incident/emergency reporting, 210
 - Kick-off agenda sample, ISA project management, 65
 - Kick-off memo sample, ISA project management, 63–64
- L**
- LANs, *see* Networks/LANs/WANs
 - Layered access controls, 9
 - Learning objectives
 - incident/emergency response, 201–203
 - policies, standards and procedures, 77–81
 - Legal counsel
 - evolution of role, 35
 - organization/infrastructure components, 28, 37–39
 - Legal/regulatory issues, 94–95, 295–296
 - baselines and risk assessments, 103
 - copyrights and licensing compliance, 107
 - e-mail, 85–86
 - external audit, 41
 - incident/emergency response, 234–235
 - legal counsel, responsibilities of, 37–38
 - policies, standards and procedures, 77, 79, 85–86
 - violations of policy, policy sample, 246

INFORMATION SECURITY ARCHITECTURE

Legislation, 94–95
Liaison, network and application
 administrator responsibilities, 37
Liaisons, security, *see* Security coordinators
 or liaisons
Library, media, 168
Library control systems, change
 management, 117
Licenses and copyright compliance, 107, 252
Licensing, software, line of business (LOB)
 security plan, 345
Life cycle, security, 176–177, 240
Line of business (LOB) security plan
 compliance, 173
 sample, 337–364
 executive summary, 338–340
 firewall, 358–359
 glossary, 364
 Internet review, 353–357
 LAN assessments, 340–346
 LAN/WAN gateway review, 346–353
 routers, 357–358
 UNIX server, 359–360
Local area networks (LANs), *see*
 Networks/LANs/WANs
Local security authority (LSA), 129, 130
Lockouts
 log on failures, 115
 voice mail, 136
Log files, incident/emergency response, 216,
 217–218, 222
Logging
 line of business (LOB) security plan,
 361–362
 problem management, 111
Logical security
 audits, 168
 microcomputer security, 107
Log-on
 enterprise management tools, 174
 secure attention sequence, 130
Log-on failures
 lockouts, 115
 voice mail, 136
Lotus mail servers, 284

M

Magazines, security, 153–154
Mail technology
 e-mail, *see* E-mail
 enterprise management tools, 174
Main distribution facilities (MDFs), 135

Maintenance, application development and
 implementation, 116, 117
Malicious code, 213
Management, *see also* Executive
 management
 application development and
 implementation, 116
 baselines and risk assessments, 102
 information security architecture project,
 56
 network security assessment workplan,
 311–312
 organization/infrastructure, 26
 organization/infrastructure components,
 28
 pitfalls of effective ISA program, 198
 policies, standards and procedures, 79
 policy objectives, 246
 telecommunications security
 assessment, 328–329
Management buy-in, incident/emergency
 response, 231
Management tools,
 organization/infrastructure, 37–38
Mandatory access control (MAC) systems,
 127
Manual, policy, 243–257
Manual, standards and procedures, 277–281
 ISA project deliverables, 71
 policies, standards and procedures, 95,
 97
 strategic information technology (IT)
 plan, 20
Media library management, 168
Mergers and acquisitions
 pitfalls of effective ISA program, 198
 security program pitfalls, 183–186
Messages, security, 155–156
Microcomputer security
 assessment workplan, 294–295
 baselines and risk assessments, 103, 107
Microsoft, corporate espionage, 144
Microsoft service packs, Windows NT, 131
Mission-critical systems, awareness and
 training program, 161
Mission statement, CSIRT, 226–227, 228
Mobile communications, 132
Mom-and-pop shop beginnings, pitfalls of
 effective ISA program, 191–192
Monitoring and detection
 architecture, 75
 assessment workplan, 293–294
 baselines and risk assessments, 103
 components of internal control, 167

- continuous, 197
- contractors and third-party vendors, 195
- e-mail policy enforcement, 87
- line of business (LOB) security plan, 361–362
- policy manual sample, 254
- strategic information technology (IT) plan, 52
- MS/DOS, 128, 130
- Multimedia presentations, 155

N

- National Computer Security Center (NCSC) rating, Windows NT, 126–127
- National Infrastructure Protection Center (NIPC), 156
- National Security Agency (NSA), evaluation and certification of systems, 127, 128
- Network administrators, compliance/control implementation, 166–167, 177
- Network management tools, contractors and third-party vendors, 195
- Networks/LANs/WANs, 50
 - access points, 9–11
 - architecture, 8, 9
 - baselines and risk assessments, 102, 119–120
 - e-mail and virtual office, 123–124
 - gateways separating corporate WAN and lines of business, 122
 - operating system, 125–132
 - placement of WAN resources at client sites, 124–125
- chief information officer responsibilities, 31
- client-server environments, 8
- computing policy, 263–265
- incident/emergency response, containment, 222
- line of business (LOB) security plan
 - executive summary, 338–339
 - LAN assessments, 340–346
 - LAN/WAN gateway review, 346–353
- merger/acquisition impact analysis, 185
- organization/infrastructure, 26
- organization/infrastructure components, 37
- ownership of information and resources, 48
- piecemealing, 10
- policies, standards and procedures, 82–83

- security assessment workplan, 309–319
 - access controls, 312–313
 - backup and recovery, 316
 - external access, 316
 - hardware/software/circuits, 315–316
 - Internet, 316–317
 - management, 311–312
 - operating environment, 309–311
 - remote access, 314–315
 - third-party providers, 314
- security program pitfalls, mainframe personnel, 188–189
- strategic information technology (IT) plan, 18
- strategic information technology (IT) plan questions, 22
- Windows NT, 131
- Windows NT assessment workplan, 325
- New applications, chief information officer responsibilities, 29
- New employees
 - awareness and training program, 150, 155–156
 - security coordinator or liaison responsibilities, 36
- Newsletters
 - professional organizations, 160
 - security awareness training, 158–159
- New systems design controls, 168
- New technology, 242
- Newton's Telecom Dictionary*, 8
- NIPC (National Infrastructure Protection Center), 221
- Noncompliance, policy manual sample, 251
- Nonrepudiation, 15, 247
- Notification
 - contractors and third-party vendors, 195
 - emergency response plan, 333, 335–336
 - incident/emergency response, 208, 209, 224–226
- NS lookup, 222

O

- Object integrity, enterprise management tools, 174
- Objectives, business, *see* Business objectives
- Objectives, IT security
 - policy manual sample, 246–247
 - strategic information technology (IT) plan questions, 23
- Object-oriented (OO) architectures, 129, 131
- Object reuse, 130

INFORMATION SECURITY ARCHITECTURE

- Open processing environments, defined, 7
- Operating environment
 - assessment workplan, 287–289
 - baselines and risk assessments, 102
 - component identification, 47
 - network security assessment workplan, 309–311
- Operating system, *see also* Windows NT
 - assessment of security, 125
 - merger/acquisition impact analysis, 185
 - organization/infrastructure, 26
 - policies, standards and procedures, 95
- Operational security programs
 - assessment workplan, 293–296
 - compliance with legal and regulatory requirements, 295–296
 - microcomputer security, 294–295
 - security monitoring, 293–294
 - virus controls, 294
- Operations, *see* Computer operations; Security operations
- Organizational hierarchy, security officer place in, 33
- Organizational processes, awareness and training program, 162
- Organization chart
 - baselines and risk assessments, 102
 - merger/acquisition impact analysis, 185
- Organization/infrastructure, security, 25–75
 - assessment workplan, 289–290
 - audits, 39–42
 - compliance, 42
 - component, 42
 - external, 41–42
 - internal, 39–41
 - baselines and risk assessments, 102
 - centralized versus decentralized security administration, 43–45
 - components
 - chief financial officer, 31–32
 - chief information officer, 29–31
 - departmental management, 36–37
 - executive committee for security, 29
 - human resources, 37
 - legal counsel, 37–39
 - network and application administrators, 37
 - security coordinators or liaisons, 35–36
 - security officer, 32–33
 - security team, 33–34
 - emergency response plan, 332–333
 - ISA deliverables, I, 71–75
 - ISA project management, 56–71
 - announcement letter sample, 57–58
 - binder labels, suggested, 66
 - charter sample, 58–62
 - interview schedule, 67
 - interview template, 68
 - kick-off agenda sample, 65
 - kick-off memo sample, 63–64
 - status report, 69, 70–71
 - task tracking spread sheet, 68
 - learning objectives, 25–26
 - line of business (LOB) security plan, 350
 - strategic information technology (IT) plan, 49–50
 - system users, 42–43
 - telecommunications security assessment, 327–328
- Organizations, professional, 154
 - incident/emergency response, 220–221
 - security awareness training, 159–160
- Outsourced services, *see* Third-party vendors and service providers
- Owner, component
 - defining, 47
 - responsibilities for, 35
- Owner security ID, 129
- Owners/ownership
 - and access controls, 112–113
 - application, appropriate operation definition, 4–5
 - compliance/control implementation, 165
 - component
 - compliance, 166–167
 - defining, 47
 - responsibilities for, 35
 - enterprise management tools, 175
 - ISA project deliverables, 71, 72
 - line of business (LOB) security plan, 349–350
 - organization/infrastructure, 46, 47, 48
 - policies, standards and procedures, 80, 98
 - policy manual sample, 251, 252

P

- Partnerships, chief information officer responsibilities, 30
- Password parameters, 72–75
- Passwords
 - authentication, 114–115
 - awareness and training program, 146, 150
 - changing, 150

- contractors and third-party vendors, 194, 195–196
- enterprise management tools, 174
- incident/emergency response, 223–224
- issues discussion document example, 72–73
- line of business (LOB) security plan, 362, 363
- organization/infrastructure, 26
- policy objectives, 247
- private branch exchanges (PBX), 135
- system user security responsibilities, 42
- voice mail, 136
- Windows NT assessment workplan, 324
- Patches, security officer responsibilities, 32
- Peripherals, controls, 169
- Permissions, enterprise management tools, 175
- Personnel, *see also* Employees; Human resources
 - information security policy
 - acknowledgment form, 259–261
 - new employees
 - awareness and training program, 150, 155–156
 - security coordinator or liaison responsibilities, 36
 - security organization components, 28
 - chief financial officer, 31–32
 - chief information officer, 29–31
 - executive committee for security, 29
 - help desk, 39
 - human resources, 37
 - security coordinators or liaisons, 35–36
- Phased approach, security assessment
 - baselines and risk assessments, 102–103
 - computer operations (section III), 102–111
 - backup and recovery, 109–110
 - computer systems management, 110
 - physical and environmental security, 108–109
 - problem management, 110–111
 - high-level (section I), 103–105
 - organization of security function, 103
 - policies, standards, 104
 - risk-related programs, 104–105
 - security plan, 104
 - security operations (section II), 105–107
 - compliance with legal and regulatory requirements, 108
 - computer virus controls, 106
 - microcomputer security, 107
 - security monitoring, 105–106
- Phone card charges, 133
- Physical and environmental security
 - assessment workplan, 296–297
 - baselines and risk assessments, 103, 108–109
 - controls, 168
 - microcomputer security, 107
 - strategic information technology (IT) plan questions, 23
 - types of controls, 15, 16, 17
 - types of threats, 12
 - WAN placement at client sites, 124–125
- Physical controls, 15, 16, 17
- Ping, 222
- Pitfalls to effective ISA program, 179–199
 - discord between mainframe versus distributed computing cultures, 188–189
 - executive-level responsibilities, 180–181
 - executive management's lack of understanding of realistic risk, 181–182
 - fostering trust in organization, 190–191
 - impact of mergers and acquisitions on disparate systems, 183–186
 - independent operations throughout business units, 186–188
 - lack of a project sponsor and executive management support, 180–181
 - lack of resources, 182–183
 - mom-and-pop shop beginnings, 191–192
 - rate of change in technology, 196–197
 - third-party and remote network management, 192–196
- Plain old telephone system (POTS), 132
- Planning
 - baselines and risk assessments, 102
 - business, *see* Strategic business plan
 - chief information officer responsibilities, 29
 - emergency response plan, 332
 - strategic information technology (IT) plan, *see* Strategic information technology (IT) plan
- Policies, standards, and procedures, 77–99
 - administrative controls, 134
 - architecture, 75
 - assessment workplan, 291–292
 - awareness and training program, 161
 - baselines and risk assessments, 102
 - chief information officer responsibilities, 29

INFORMATION SECURITY ARCHITECTURE

- compliance checks, 6
- components, 81–82
- development of, 98–99
- e-mail policy, 83–87
- firewall selection incident, 4–5
- human resources, responsibilities of, 37
- incident/emergency reporting, 210
- information security policy, 81–82
- information security policy
 - acknowledgment form, 82
- Internet policy, 87–89
- Internet risk, 88–89
- ISA project deliverables, 71
- learning objectives, 77–81
- legal counsel, responsibilities of, 37
- merger/acquisition impact analysis, 185
- network usage policy, 82–83
- process for change, 90–91
- samples
 - anti-virus update procedure, 283–285
 - e-mail security, 267–269
 - Internet, 271–273
 - network computing, 263–265
 - policy manual, *see* Policy manual (sample)
 - security standards and procedures
 - table of contents, 277–281
- security officer responsibilities, 32–33
- security procedures, 96–97
- security standards, 91–92
- security team responsibilities, 34
- standards organizations, 92–95
- strategic information technology (IT)
 - plan, 20, 52
- strategic information technology (IT)
 - plan questions, 23
- system user security responsibilities, 42
- types of controls, 15, 16, 17
- Policy development, incident/emergency response, 233–234
- Policy manual (sample), 243–257
 - controls, 255–257
 - implementation, 251–255
 - policy, 245–251
 - information security, 245–246
 - objectives, 246–247
 - scope and responsibilities, 247–251
 - table of contents, 244
- Politics, and security, 187
- Power Point presentations, 155
- Preventive controls, 16–17
- Previous assessment/audit reports,
 - baselines and risk assessments, 102

- Private branch exchanges (PBX), 132
 - administrative controls, 135
- Proactive services, incident/emergency response, 204–205
- Probe, incident/emergency response, 213
- Problem management
 - assessment workplan, 299
 - baselines and risk assessments, 103, 110–111
 - contractors and third-party vendors, 195
- Procedures, *see also* Policies, standards, and procedures
 - defined, 78
 - learning objectives, 77
 - manual, *see* Manual, standards and procedures
 - policies, standards and procedures, 96–97; *see also* Policies, standards, and procedures
- Process for change, policies, standards and procedures, 90–91
- Processing environment
 - organization/infrastructure, 26
 - pitfalls of effective ISA program, 198
 - strategic information technology (IT)
 - plan questions, 22, 23
- Production libraries, application development and implementation, 116
- Program considerations, awareness and training program, 147–160
- Program development, awareness and training program, 161–162, 163
- Program objectives, awareness and training program, 139–147
- Project management, ISA, 56–71
 - announcement letter sample, 57–58
 - awareness and training program, 151–152
 - binder labels, suggested, 66
 - charter sample, 58–62
 - interview schedule, 67
 - interview template, 68
 - kick-off agenda sample, 65
 - kick-off memo sample, 63–64
 - status report, 69, 70–71
 - task tracking spread sheet, 68
- Publications, security, 153–154
- Purchase decisions, chief information officer responsibilities, 30

Q

- Quality assurance parameters,
 - incident/emergency reporting, 210

- Quality management services,
 - incident/emergency response, 205
- Queues, enterprise management tools, 175
- Quick Response (QR), 18, 50
- R**
- RACF, 113
- Raffles, 156–157
- Rate of change in technology, pitfalls of
 - effective ISA program, 196–197
- Reactive services, incident/emergency response, 205–208
 - alerts and warnings, 205–206
 - artifact handling, 207–208
 - goals and responsibilities, 204, 205
 - incident handling, 206–207
 - vulnerability handling, 207
- Recording test, application controls
 - assessments, 169–170
- Record keeping, problem management, 111
- Recovery, incident/emergency response, 208, 209, 215, 224
- Reduced instruction set computers (RISC), Windows NT, 126
- Reevaluation of CSIRT operations,
 - incident/emergency response, 236
- Reference documents
 - operating environment component identification, 47
 - ownership of information and resources, 48
- Refresher training, 150
- Regulatory and legal issues, *see*
 - Legal/regulatory issues
- Remediation, baselines and risk assessments, 104
- Remote access, 9
 - administrative controls, 135–136
 - baselines and risk assessments, 121
 - client-server environments, 9
 - line of business (LOB) security plan, 351–353
 - network security assessment workplan, 314–315
 - ownership of information and resources, 48
 - strategic information technology (IT)
 - plan questions, 22
 - Windows NT assessment workplan, 324
- Reports/reporting
 - awareness and training program, 142–143, 161
 - baselines and risk assessments, 102
 - chief financial officer responsibilities, 31
 - controls, 169
 - emergency response plan, 334–335
 - enterprise management tools, 174
 - incident/emergency response, 209–213
 - incident handling, 206
 - incident response, 218–219
 - methodology, 209
 - system user security responsibilities, 42
 - telecommunications security
 - assessment, 327–328
- Request for comment, policies, standards and procedures, 77, 97–98
- Research and development, security, 45
- Resource, information, implementation, 251–252
- Resource commitment, *see also*
 - Funding/budget
 - awareness and training program, 147–148
 - pitfalls of effective ISA program, 182–183
- Resource ownership, ISA project
 - deliverables, 71, 72
- Response, incident/emergency response, 206–207, 208
- Responsibility, 240–241
 - administrative controls, 134
 - compliance/control implementation, 165
 - job description, description in, 140
 - merger/acquisition impact analysis, 185
 - policy manual sample, 247–251
 - strategic information technology (IT)
 - plan questions, 22
- Restricted access, application control
 - objectives, 169
- Risk assessment, *see also* Baselines and risk assessments
 - assessment workplan, 292–293
 - policy manual sample, 255–256
- Risk-based approach to auditing, 170
- Risks
 - controls overview, 12–14
 - external audit, 41
 - Internet policy, 88–89
 - issues discussion document example, 73–74
 - organization/infrastructure, 26
 - policies, standards and procedures, 80
 - security life cycle, 176
 - security officer responsibilities, 32
 - security team responsibilities, 34, 35
 - strategic information technology (IT)
 - plan questions, 22, 23
- Role-based access, 112
- Root-kit attack, 223

INFORMATION SECURITY ARCHITECTURE

Router access and configuration,
 contractors and third-party
 vendors, 195
Routers, 8
 incident/emergency response, 223–224
 line of business (LOB) security plan,
 357–358
 ownership of information and resources,
 48

S

Scalability, enterprise management tools,
 173–174
Scope of policy, 247–248
Secure attention sequence
 (Control–Alt–Delete), 130
Secure token, 115
Security account manager (SAM), 129, 130
Security advisory committee, 35
Security assessment workplan, 287–299
Security coordinators or liaisons, 45
 access controls, 46–47
 awareness and training program, 146
 incident/emergency reporting, 210
 organization/infrastructure components,
 28, 35–36
 responsibilities, policy manual sample,
 248–249
Security days, 156
Security lists, 275–276
Security monitoring, baselines and risk
 assessments, 105–106
Security officer
 awareness and training program, 146,
 151–152
 compliance audits, 42
 organization/infrastructure components,
 28, 32–33, 34
 responsibilities, policy manual sample,
 248
Security operations
 baselines and risk assessments, 105–107
 compliance with legal and regulatory
 requirements, 108
 computer virus controls, 106
 microcomputer security, 107
 security monitoring, 105–106
 CSIRT, reevaluation of, 236
Security organization, *see*
 Organization/infrastructure,
 security
Security organizations, professional, *see*
 Organizations, professional
Security policy, *see* Policies, standards, and
 procedures
Security procedures, 96–97; *see also* Policies,
 standards, and procedures
Security standards, 91–92; *see also* Policies,
 standards, and procedures
Security team
 centralized versus decentralized security
 administration, 43–44
 compliance, 172–173
 compliance audits, 42
 compliance/control implementation,
 165–166
 compliance testing, 177
 organization/infrastructure components,
 28, 33–34
 policies, standards and procedures, 79,
 98, 99
 responsibilities, policy manual sample,
 249
 security officer responsibilities, 32
Separation/segregation of duties, baselines
 and risk assessments, 113–114
Servers, line of business (LOB) security plan,
 359–360
Service packs, Windows NT, 131
Session controls, application development
 and implementation, 116
Signature, digital, 15–16
Size of enterprise,
 organization/infrastructure, 26
Slogans, security, 155–156
Sniffing, 213
Software, 242
 access control, 113, 170
 client-server environments, 8
 enterprise management tools,
 173–176
 incident/emergency response, 216
 keystroke recording, 150
 network security assessment workplan,
 315–316
Software development, microcomputer
 security, 107
Source libraries, application development
 and implementation, 116
Sponsorship
 information security architecture project,
 56
 pitfalls of effective ISA program, 180–181
Staffing and training, incident/emergency
 response, 231–232
Standard operating procedures
 compliance audits, 42

- component audits, 42
 - incident/emergency response, 222–223
 - Standards
 - defined, 78
 - learning objectives, 77
 - manual, *see* Manual, standards and procedures
 - policies, standards and procedures, 91–92; *see also* Policies, standards, and procedures
 - Standards organizations, 77, 92–95, 97–98
 - Startup files, enterprise management tools, 174
 - Status report, ISA project management, 69, 70–71
 - Strategic business plan
 - chief financial officer responsibilities, 31
 - resource allocation, 182–183
 - strategic information technology (IT) plan and, 19, 20
 - strategic information technology (IT) plan questions, 23
 - Strategic goals for IT
 - chief information officer responsibilities, 30
 - strategic information technology (IT) plan and, 19
 - Strategic information sources, awareness and training program, 161
 - Strategic information technology (IT) plan architecture, 17–22
 - description of organization, 18
 - integrated framework, 20, 21
 - overview/executive summary, 18
 - relationship to organization's strategic business plan, 19
 - scope, viability, and modification of plan, 18–19
 - strategic goals for information technology, 19
 - chief information officer responsibilities, 29
 - components, 51–54
 - organization/infrastructure, 26
 - Strategic planning, chief financial officer responsibilities, 31
 - Subcontractors, *see* Contractors; Third-party vendors and service providers
 - Suppliers, chief information officer responsibilities, 30
 - System access control list (SACL), 129, 131
 - System administrators, awareness and training program, 146, 154
 - System configuration, Windows NT
 - assessment workplan, 321–322
 - System identity, incident/emergency response, 223–224
 - System management, baselines and risk assessments, 103
 - System queues, enterprise management tools, 175
 - Systems environment,
 - organization/infrastructure, *see* Organization/infrastructure, security
 - Systems management, assessment workplan, 297
 - Systems programmers, change management, 117
- ## T
- Target audience, awareness and training program
 - reaching, 154–159
 - scoping, 149–154
 - Task tracking spread sheet, ISA project management, 68
 - Team, security, 28, 33–34
 - Technical controls, 15–16
 - Technical procedure announcements, 225
 - Technical support, incident/emergency response, 216
 - Technology
 - chief information officer responsibilities, 29, 30
 - telecommunications security assessment, 327
 - Telecommunications, *see also* Communications
 - networks/technologies
 - administrative controls, 133–135
 - assessments, 132–136
 - assessment workplan, 327–330
 - changing technology, 196
 - Telecommuting, 18, 50
 - Teleconferencing, 132
 - Telephone charges, 132–133
 - Telephone logs, 135
 - Telephones, 132
 - Telnet, 222
 - Temporary employees
 - corporate espionage, 143–144
 - security procedures, 162
 - Temporary fixes, application development and implementation, 117

INFORMATION SECURITY ARCHITECTURE

Third-party vendors and service providers,
 see also Contractors
 administrative controls, 134–135
 network management, 192–196
 network security assessment workplan,
 314
 security procedures, 162

Threats
 controls overview, 11–12
 strategic information technology (IT)
 plan questions, 22

Timelines, contractors and third-party
 vendors, 195

Tools, awareness and training program, 161

Top Secret (access control software), 113

Tracing, incident/emergency response,
 206–207, 208, 209

Tracking, incident/emergency response,
 206–207, 208, 209

Tracking number, incident/emergency
 reporting, 210, 214

Training
 chief information officer responsibilities,
 30
 incident/emergency response, 231–232
 microcomputer security, 107
 security awareness, 5–6; *see also*
 Awareness and training program

Transfers, employee, 150

Triage, 209, 213–215

Trojan horses, 88, 130, 213, 217

Trusted computing base (TCB), Windows NT,
 128

U

Unauthorized access, *see*
 Incident/emergency response

Unauthorized software, 107

Uninterrupted power supplies, 108

United States Computer Emergency
 Response Team (US-CERT), 221

UNIX, 48

UNIX server, line of business (LOB) security
 plan, 359–360

Updates, security officer responsibilities, 32

Usage policies, microcomputer security, 107

User identification
 contractors and third-party vendors, 194
 integrity of system, 1
 organization/infrastructure, 26

User mode, Windows NT, 128

User permissions, enterprise management
 tools, 175

Users
 awareness and training, *see* Awareness
 and training program
 implementation, policy manual sample,
 252
 information security policy
 acknowledgment form, 259–261
 organization/infrastructure components,
 28
 responsibilities, policy manual sample,
 251

User's group, 28

V

Validation, user, 194

Validity, application control objectives, 169,
 170

Vendors
 maintenance of lists, 113
 service providers, *see* Third-party
 vendors and service providers

Version releases and updates, security
 officer responsibilities, 32

Videos, security training, 140–142, 155

Videotape, chain of custody documentation,
 216

Violations of company policy
 e-mail, 269
 policy manual sample, 246

Virtual office, baselines and risk
 assessments, 123–124

Viruses/anti-virus procedures, 13, 88
 assessment workplan, 294
 awareness and training program, 153
 baselines and risk assessments, 103, 106
 incident/emergency response, 213
 line of business (LOB) security plan,
 345–346
 merger/acquisition impact analysis, 185
 security procedures, 96–97
 strategic information technology (IT)
 plan questions, 23
 types of threats, 12

Visitors, security procedures, 162

Voice mail systems, 132, 136, 185

Vulnerabilities
 incident/emergency response, 207
 testing, 5

W

WANs, *see* Networks/LANs/WANs

- War dialing, 213
- Web sites
 - policies, standards and procedures
 - information, 95
 - policy distribution, 90
 - security officer responsibilities, 32
- Wide area networks (WANs), *see*
Networks/LANs/WANs
- Windows administrator, security
 - coordinator or liaison
 - cooperation, 47
- Windows environments, ownership of
 - information and resources, 48
- Windows NT, 48
 - assessment workplan, 321–325
 - baselines and risk assessments, 125–132
- Windows NT file system (NTFS), 130
- Windows XP, 48
- Workflow technology, 18, 50
- Workplan
 - assessment, 287–299; *see also*
Assessment workplans
 - information security architecture project,
104
- Worms, 213

Jan Killmeyer

Information Security Architecture

An Integrated Approach to Security in the Organization
Second Edition

Information Security Architecture: An Integrated Approach to Security in the Organization, Second Edition simplifies security by providing clear and organized methods and by guiding you to the most effective resources available.

In addition to the components of a successful Information Security Architecture (ISA) detailed in the previous

edition, this volume also discusses computer incident/emergency response. The book describes in detail every one of the ISA components. Each chapter provides an understanding of the component and details how it relates to the other components of the architecture. The text also outlines how to establish an effective plan to implement each piece of the ISA within an organization.

The second edition has been modified to provide security novices with a primer on general security methods. It has also been expanded to provide veteran security professionals with an understanding of issues related to recent legislation, information assurance, and the latest technologies, vulnerabilities, and responses.

Features:

- Provides executives with an understanding of the requirements of a strategic security plan
- Defines laws and regulations related to electronic transmissions, computer crime, intellectual property, information protection, and privacy
- Reviews the pitfalls and obstacles to effective ISA implementation
- Addresses security technology including encryption, firewalls, VPNs, passwords, biometrics, honeypots, and more
- Includes a “Getting Started” section in each chapter to help you build ISA components

AU1549

ISBN 0-8493-1549-2



Auerbach Publications

Taylor & Francis Group

www.taylorandfrancisgroup.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
270 Madison Avenue
New York, NY 10016