Nonprofit Risk Management Center

Vol. 22, No. 1, Spring 2013

Risk Management ESSENTIALS

Tips, Knowledge and Tools for Nonprofit Organizations

2013 Risk SUMMIT

August 25 – 27, 2013
Revere Hotel – Boston, MA

We invite you to attend the *2013 Risk SUMMIT* at the Revere Hotel in Boston. During this three day event, you will enjoy provocative keynotes, enlightening risk management workshops, a vendor expo, and the chic ambience of the Revere Hotel.

The Revere is a modern, eccentric hotel in the Back Bay neighborhood, only a block from scenic Boston Common and a short walk from the historic South End neighborhood. Back Bay is home to countless 19th century Victorian homes and the beautiful Boston Public Library. The Revere is within walking distance of prime Boston sights including: Paul Revere's house, Trinity Church, Fenway Park, New England Aquarium, the Boston Public Gardens, and the local shopping hotspot of Newbury Street.

To register for the SUMMIT, visit www.nonprofitrisk.org/summit.

The Tech Issue

Risk in the Cloud

by Erin Gloeckner

Remember the craze over beanie babies in the 1990s? I was just a kid during the 90s, so I innocently endorsed that craze. My parents suffered through my childhood, spending heaps of money when I demanded to have the next bear, skunk, or whale in my collection. Dozens of cute, colorful animals named 'Binksy' or 'Bubbles' littered my bedroom bookshelf. Beanie babies were a money pit and I didn't even know how to play with them. You might feel the same way about technology fads; you spend half a paycheck on the latest gadget, and feel duped when it winds up collecting dust on a shelf.

The latest buzzword in the world of technology is 'cloud computing.' Cloud computing has existed for more years than many nonprofit leaders realize. But leaders are only recently starting to think about risk when they contemplate the rewards of embracing the cloud.

What Does 'Cloud' Mean, Anyway?

The term 'cloud' is used to describe any service that is housed by a vendor instead of residing on the servers of the organization using the application

continued on page 2

A publication of the
Nonprofit Risk Management Center
©2013 Nonprofit Risk Management Center
15 N. King Street, Suite 203 • Leesburg, VA 20176 • Phone: (202) 785-3891 • Fax: (703) 443-1990 • www.nonprofitrisk.org

Risk Management
ESSENTIALS
Vol. 22 • No. 1 • Spring 2013
Published three times annually by the
Nonprofit Risk Management Center
15 N. King Street, Suite 203
Leesburg, VA 20176
Phone: (202) 785-3891
Fax: (703) 443-1990
Web site: www.nonprofitrisk.org.

Nonprofit Risk Management Center

Staff Directory

(All staff can be reached at 202.785.3891)

Melanie Lockwood Herman
■ *Executive Director*
Melanie@nonprofitrisk.org

Erin Gloeckner
■ *Project Manager*
Erin@nonprofitrisk.org

Sue Weir Jones
■ *Office Manager*
Sue@nonprofitrisk.org

Jennifer Walther
■ *Director of Client Solutions*
Jennifer@nonprofitrisk.org

2013 Board of Directors

President
Michael A. Schraer
Chubb & Son
Warren, NJ

Treasurer
Lisa Prinz
Harleysville Insurance
Harleysville, PA

Secretary
Carolyn Hayes-Gulston
National Multiple Sclerosis Society
New York, NY

Peter Andrew
Council Services Plus, Inc.
Albany, NY

David S. Kyllo
Riverport Insurance Company
Minneapolis, MN

Robert O'Leary
Philadelphia Insurance Companies
Boston, MA

Kim Y. St. Bernard
Girl Scouts of the USA
New York, NY

Trish Shanahan
First Nonprofit Foundation
Savannah, GA

Bill Tapp
College of Direct Support
Knoxville, TN

Jeffrey D. Weslow
Housing Authority Insurance Group
Cheshire, CT

Risk in the Cloud
continued from page 1

or service. For example, the company Rackspace provides data storage infrastructure; Rackspace owns an inventory of servers with rentable space available for clients who need to store digital data. As a Rackspace customer, your nonprofit stores digital data on distant servers instead of storing on the equipment in your own building. Your data is therefore in the cloud.

'Cloud' is also used to describe software and platforms. You can use cloud software instead of installing software on your computer. Google Apps provides cloud software including Google Docs, Gmail, and Google Calendar. Instead of using calendar software that is located on your computer's hard drive, you can use Google Calendar, which is hosted by Google on a far-away server. You never have to download it to use it; you simply log in to the cloud-application hosted by Google.

Forecast: Cloudy with a Chance of Risk

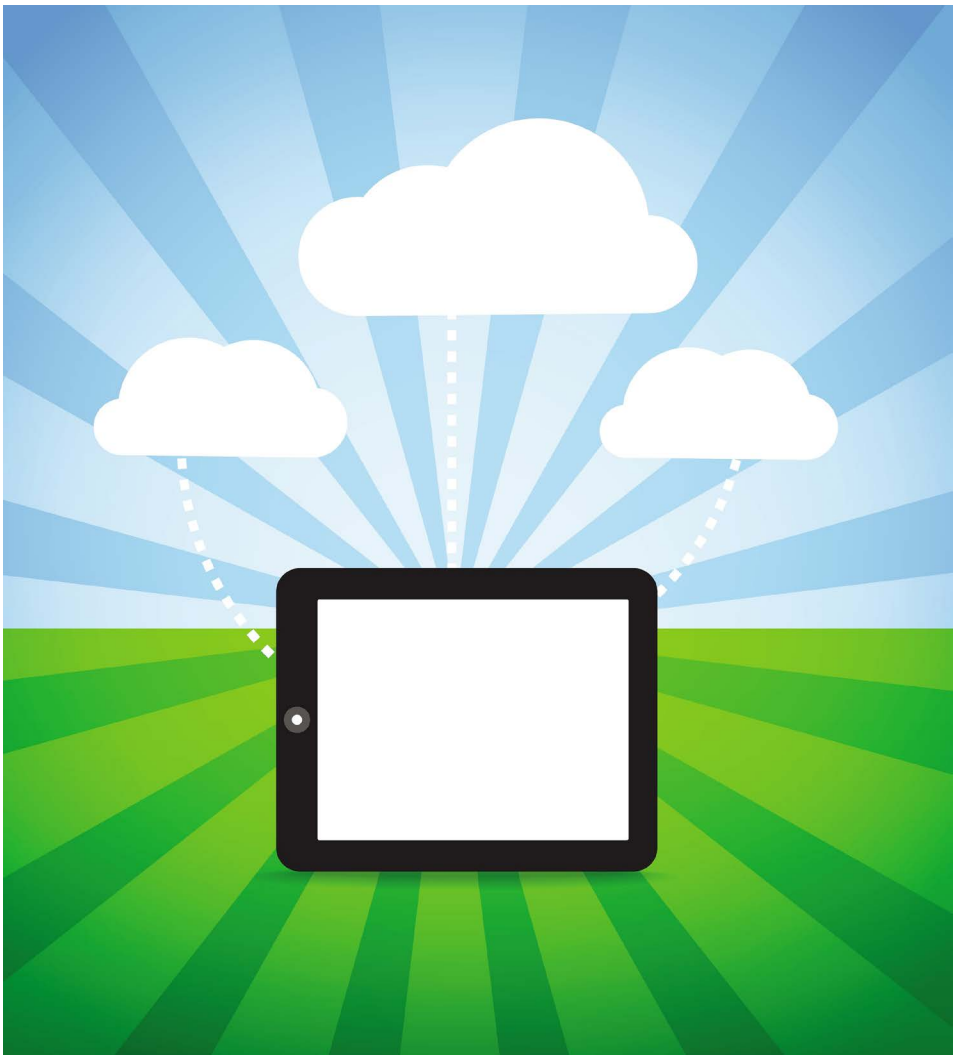
There are a wide range of risks associated with cloud computing, many of which come from user error rather than the technology itself. Yes, you should be worried about information security and data breaches from outside parties. But before worrying over risks in the cloud, make sure your feet are planted firmly on the ground.

During the March 2013 webinar on "Risk in the Cloud," hosted by the Nonprofit Risk Management Center, guests David Linthicum of Blue Mountain Labs and Matt Prevost of Philadelphia Insurance Companies explained why nonprofit leaders often stumble during their climb to the cloud. Avoid these common failures as you ascend to the cloud:

- **Falling prey to the HYPE.** David Linthicum believes that many nonprofits falter because their expectations of the cloud are unrealistic. There is so much hype surrounding the cloud that we mistakenly think cloud computing is a cure to our technology and budget woes. Instead of accepting the hype as true for your nonprofit, take the time to decide whether cloud computing opportunities are right for you. David also warns nonprofits to complete their due diligence on cloud service providers. If a provider sounds too good to be true, they may indeed be.
- **Trying to fly with NO PLANNING or EXPERIENCE.** David says another mistake nonprofits make is embracing cloud services and applications without vital technical knowledge or experience. If your nonprofit doesn't have a tech-wiz on staff, then David suggests you get help from an expert. He also encourages nonprofits to complete a few key steps before transitioning to the cloud:
  - ❑ Test your new cloud technology on one system before moving everything to the cloud.
  - ❑ Consider testing a non-critical system first, rather than testing your cloud with data that is critical to your mission.
  - ❑ Contemplate how the cloud will impact and integrate into existing structures and processes at your nonprofit.
  - ❑ Recognize the cloud's impact on your core strategies as well as existing security protocols.
- **Failing to anticipate the risk of DATA BREACHES.** Matt Prevost warns us to focus on safeguarding

continued on next page

Risk in the Cloud
continued from page 2



> Don't assume that existing property and casualty policies will cover new exposures arising from your activity in the cloud.

specific information stored in the cloud, namely: personal health information, personally identifiable information, financial information, and intellectual property. Be sure to protect the information of your clients and donors as well as that of your employees, board members, and volunteers.

Before you choose to abandon some or all of your in-house servers or installed applications, take the time to understand the protection from financial losses available through cyber insurance policies. Most importantly, **don't assume that existing property and casualty policies will cover new exposures arising from your activity in the cloud.** Matt explains that most traditional property, liability, and crime policies do not cover damage to data and cyber systems. Your nonprofit may require cyber insurance to cover losses including: cyber extortion, business interruption due to digital malfunction, loss of digital assets, loss of electronic intellectual property, or a compromise of network privacy or employee privacy. Luckily, some cloud service providers also offer cyber insurance. Depending on your needs, it may be more effective to purchase coverage from an outside provider.

continued on page 4

Risk in the Cloud
continued from page 3

Avoid Rain Clouds by Screening Cloud Service Providers

Never be shy about questioning cloud candidates. Before they buy in, smart nonprofit leaders compare potential cloud service providers. Ask very specific questions and check references for any new vendor. Never assume that a vendor will protect your interests financially or otherwise if they make a mistake or something goes wrong. Remember to ask the following questions of your cloud service candidates:

- What is the provider's response time when the cloud servers go down? What is the estimated 'uptime' it will take to get things working?
- Will my nonprofit still have ownership of electronic documents and property that we store in the cloud? What are our owner rights and responsibilities?
- Does the provider offer a warranty? Does the provider have limited liability if we experience a data breach or other loss?
- What is the provider's dispute resolution process?
- Has the provider acted in consistency with other agreements they have entered into?
- What are the provider's payment terms?

A Remedy for Cloud Fever

Ask yourself these questions before making the jump to the cloud:

- How is my nonprofit exposed to risks in the cloud? What are the major categories of risk?
- Have other nonprofits stumbled when moving to the cloud? How can my nonprofit keep from making the same mistakes?
- What type of cyber security options are available to protect our cloud data?
- What role might insurance play in the event a downside cyber risk materializes?
- How have other nonprofits fared after transitioning from in-house servers to cloud servers?
- Are all of our staff prepared to access information in the cloud, or are some staff at risk of being stranded on the ground?
- Is our nonprofit jumping on the cloud computing bandwagon just to keep up with the trend?
- Do we have staff members who actually understand the technical aspects of cloud computing?
- Are we prepared to experience cultural and procedural shifts as we rely more heavily on cloud services?
- Have we ever felt disenchanted after adopting the latest IT craze? Why wasn't the previous technology craze useful to us?
- What are our requirements? What systems do we want to move to the cloud? Do we want infrastructure, a platform, software, a network, or all of those things from a cloud provider?

Erin Gloeckner is Project Manager at the Nonprofit Risk Management Center. She recently moderated a webinar on cloud risks. Erin welcomes your feedback and questions about any of the topics addressed in this article at Erin@nonprofitrisk.org or (202) 785-3891.

Insurance for Cyber Risks

By Melanie Lockwood Herman

Today's nonprofit leaders are aware that dependence on data, software, systems and tech vendors brings untold benefits as well as potential downside risks. From the impact of data loss to claims alleging the failure to safeguard personal information, a nonprofit's reputation and resources are 'on the line' in the online age. Effective risk assessment and risk management can help an organization's leaders feel confident that appropriate steps have been taken to minimize the likelihood of a downside risk. Strong risk protocols and preparation can instill confidence that the nonprofit will do the right thing should a data loss, breach of privacy claim, or vendor error occur.

Once risk assessment and risk management are in place, it's time to consider risk financing: how will we pay for the cost of losses and harm we're unable to avoid?

During the March 2013 webinar on "Cloud Computing Risks," hosted by the Nonprofit Risk Management Center, Matt Prevost, AVP of Cyber and Professional Liability at Philadelphia Insurance Companies provided expert commentary on the insurable exposures related to cloud computing and storage. Matt's comments covered factors that underwriters consider in underwriting cyber coverage, as well as common mistakes that nonprofit insureds make when they migrate to the cloud. Matt graciously agreed to answer some follow-up questions, to help RME readers understand the nuances of cyber exposures and coverage.

MELANIE. *Matt, you mentioned in the webinar that nonprofit insurance buyers often make potentially dangerous assumptions when they rent server space from a cloud company. In your*

continued on page 6

Insurance for Cyber Risks
continued from page 5

experience, what are the most common assumptions, and why are they dangerous?

MATT. In some cases, nonprofits that elect to outsource data storage assume that the security somewhere else is better than what they currently have. That may be the case, but often times is not. The other wrong assumption is that the contractual relationship between the nonprofit and the technology provider adequately protects the nonprofit. These contracts often shift responsibility to the nonprofit rather than the technology provider. Additionally, within these contracts, the technology provider has minimal risk for regulatory or legal compliance, because the nonprofit retains full responsibility for the data it owns and stores. One exception is personal health information. Technology providers are now finding themselves subject to the expectations of HIPAA as business associates.

MELANIE. *During the webinar you explained that nonprofits can purchase coverage for costs they incur in the wake of a data loss/privacy breach ("first party losses") as well as losses suffered by others for which the nonprofit may be liable ("third party losses"). Is it possible to buy a policy that addresses both coverages or are separate policies required?*

MATT. Most stand-alone cyber products are scalable. What that means is that they offer a menu of insuring agreements from which the nonprofit insured can choose. And a growing number of companies offer cyber endorsements to other coverage lines. These endorsements are typically sub-limited with relatively low limits and tend to be in line with either third party exposures or first party exposures.

> "Most stand-alone cyber products are scalable. What that means is that they offer a menu of insuring agreements from which the nonprofit insured can choose."

MELANIE. *I'm aware that Philadelphia has a very large book of nonprofit business. Can you estimate what percentage of your nonprofit customers buy cyber liability coverage?*

MATT. Without giving actual figures on Philadelphia's book, I would estimate that less than 15% of all nonprofit organizations purchase coverage. Most nonprofits are just now becoming familiar with their exposure to cyber risk. With that new awareness comes interest in the insurance products available to finance those exposures.

MELANIE. *Do you see an uptick in interest following widely publicized privacy breaches, such as the recent cases involving Sony and TJ Maxx?*

MATT. We do. At the same time, there are smaller breaches publicized almost daily in local newspapers that tend to get more attention. Small and middle market nonprofit insurance buyers can relate to those smaller breaches much better. We have seen a significant interest following recent HIPAA enforcement as well. Many types of nonprofits are covered entities under HIPAA (e.g., clinics, mental health organizations, social service organizations). As covered entities they can envision the financial burden (e.g., damages, fines and penalties) that would result from claims alleging violation of HIPAA.

MELANIE. *When nonprofit leaders ask us what coverage limit they need, we generally explain that there is no formula for determining the right limit for a particular policy. Affordability*

continued on next page

Insurance for Cyber Risks
continued from page 6

is obviously an issue, but it's hard to predict what a liability claim will cost. Since cyber-based data loss and privacy breach claims are still relatively new, I imagine there isn't a lot of data on what these claims cost generally. How should a nonprofit go about determining the appropriate coverage limit for a cyber liability policy? What deductibles are typically available for this coverage?

MATT. Many carriers, including Philadelphia Insurance Companies, have risk management resources built in to their policy premiums. Philadelphia's eRisk Hub®, powered by NetDiligence, provides potential policyholders and current policyholders with access to data breach cost calculators, notification costs calculators, as well as updates to the regulatory and legal climate.

MELANIE. *Are there any key features of coverage that affect pricing?*

MATT. Key underwriting components include: total annual revenues, the type of PII (personally identifiable information) or PHI (private health information) the nonprofit collects, the number of records, and most importantly, the level of cyber risk controls an insured has in place or is willing to implement.

MELANIE. *You mentioned during the webinar that there are more than 40 markets (insurers) that provide various forms of cyber coverage. Are there dramatic differences in policy forms, or is coverage offered on Insurance Services Office (ISO, www.iso.com) or other common forms?*

MATT. There are dramatic differences in policy forms and it is important to work with an agent or broker who understands those differences. Like with any insurance product, it is most important that the policy responds to your needs. For example, if your nonprofit doesn't have the funds to retain PR help in the wake of a data breach, a cyber policy that would cover these costs for an affordable premium is a great alternative.

MELANIE. *Last question. What approach do you recommend for getting a handle on cyber property and liability exposures? Are there a few key steps that our nonprofit readers should take?*

MATT. Awareness and preparedness. Not only awareness of how important it is to securely store data (especially the most sensitive forms of data-PHI, PII and confidential information) but also being aware that losses occur every day in both small and large organizations. Having minimum controls (typically outlined in cyber insurance applications) can prevent most privacy or data breach events, but being prepared and knowing how to react following a breach is imperative. If you're a nonprofit professional and are looking to learn more about this growing risk, reach out to your agent, broker or carrier for help.

MELANIE. Thanks for sharing your valuable insights on a truly timely and complex topic.

Melanie Lockwood Herman is Executive Director of the Nonprofit Risk Management Center. She welcomes your feedback on this article and questions about the Center's resources at Melanie@nonprofitrisk.org or (202) 785-3891. Matt Prevost is Assistant Vice President, Cyber & Professional Liability at Philadelphia Insurance Companies. Matt welcomes your questions about any of the topics in this article at Matthew.Prevost@phly.com or (610) 538-2203.

Need RISK HELP?

Sign up as an Affiliate Member of the Nonprofit Risk Management Center to access RISK HELP! Center staff provide unlimited answers to Affiliates who have questions about risk. Affiliates may call or email Center staff anytime to receive RISK HELP on any risk issue. Become an Affiliate and find the answer here!

Affiliates also receive:

- **Access to the recorded Wednesday Webinar Series (12 webinars)**
- **Access to the Webinar Vault (90+ webinars)**
- **Discounts on risk management books and cloud applications**
- **Discounts on custom webinars and on-site training**
- **25% off registration for the annual Risk SUMMIT**

To learn more about Affiliate Membership, visit www.nonprofitrisk.org/affiliates or call Jennifer Walther, at (202) 785-3891.

Personal Devices at Work

By Erin Gloeckner

Employee-owned versus organization-owned… the battle wages on. As employees, many of us prefer to use personal phones and laptops for work because they are convenient, commonsense, and a lot cooler than what the IT department provides. Nonprofits know there is no way to prevent all employees from accessing personal phones at work, so many are creating BYOD (Bring Your Own Device) policies.

On its face, BYOD sounds like a wonderful cost-savings strategy. Employee productivity rises when employees use devices they know and love, and nonprofit employers save time and money as employees cover the cost of purchasing the latest productivity gizmo. The truth is, when you permit or endorse BYOD, you're inviting new and nuanced risks into your nonprofit workplace. These risks run the gamut from privacy violations to data loss and more.

BOYD and Employee Privacy

It's important to recognize that employees may need to forfeit privacy rights in exchange for the freedom to use personal devices at work. By accessing work information on a personal device, an employee puts a nonprofit's assets and reputation at risk. Employees might lose their phones, forget to encrypt work emails, or open unsecured Wi-Fi hotspots accessible by unknown external users. Even after an employee is terminated, risk remains. A former employee could bring the personal device to a new job and leak or inadvertently share sensitive information with their new employer.

To manage BYOD risks, nonprofit leaders should implement defense strategies; unsurprisingly, many defenses reduce employee privacy. For example, nonprofit IT departments may install remote access apps on personal devices, so IT administrators

continued on next page

Smart Savings or Money Pit?

According to Cecil Lynn, electronic discovery counsel at Littler law firm, BYOD does not cut costs. Lynn estimates a typical mobile BYOD environment costs 33% more than when a company owns the devices. Lynn says BYOD programs cost more than organizational ownership of IT devices because companies lose bulk purchasing power, they provide greater tech support for personal devices, and security risks are hard to budget and often wind up costing more than imagined.

Personal Devices at Work
continued from page 8

can access information when necessary. If an employee misplaces a phone used for work, the IT administrator can access the phone remotely and delete any sensitive organizational data.

Unfortunately, when such a remote access app is installed, personal documents like photos and videos may be accessed and deleted as well. IT staff may also be required to safeguard information by blocking network access, apps, and websites on personal devices. Nonprofit employees may view these acts as breaches of privacy or personal rights.

BYOD Risks to Nonprofit Employers

Aside from data breaches or the risk of a terminated employee sharing trade secrets with new employers, top BYOD concerns arise from the employment relationship.

- Workplace safety risks: While driving, employees may talk on personal devices that are used for personal *and* work reasons.
- Labor law risks: IT safeguards protecting a nonprofit's reputation and assets may be considered unlawful surveillance of employees.
- Wage and hour risks: Personal work devices used off-the-clock for business purposes may put the nonprofit employer at risk of liability for overtime time pay.
- International risks: When employees travel abroad, border guards may access sensitive data while searching devices.

BYOD use also exposes nonprofit employers to the potential for leaked contracts, leaked client/partner information, and the risk of employees uploading materials to servers owned by other companies (e.g., through the use of cloud apps like Dropbox or Google Drive). If your nonprofit aspires to best-in-class risk management as a framework for BYOD use, consider putting the following safeguards in place:

1. Create a clear policy on BYOD rights and information security rules.
2. Train employees to protect work information accessed on personal devices.
3. Require employees to sign an agreement acknowledging their role in protecting confidential or personal information stored on or accessed by personal devices.
4. Require employees to sign an agreement acknowledging the actions and steps an in-house or outsourced IT team may take to protect information stored on or accessed by personal devices.
5. Establish a protocol for wiping work-related information from lost employee devices or when separation from employment occurs.
6. Ban employees from moving funds into or out of nonprofit bank accounts using personal devices.
7. Prohibit non-exempt employees from accessing work email or making work-related calls outside of work hours, or establish clear guidelines with appropriate accountability measures permitting work outside approved schedules.
8. Consider establishing a partnership with a mobile service provider in which the provider polices information accessed on personal devices in real-time under a security agreement.
9. Offer resources like AT&T Toggle to employees, allowing them to distinguish 'work mode' from 'personal mode' on a smartphone.

No matter how many BYOD policies you create, risk remains. An IT department charged with securing nonprofit data can offer only partial protection for data stored on devices the nonprofit doesn't own. But, even if you stick to organization-owned devices, data breaches may occur. Weigh the upsides and downsides of BYOD versus organization-owned; decide whether your nonprofit is in position to take advantage of the benefits while managing the downside risks.

Additional BYOD Questions

As you design a BYOD policy or adapt a policy to reflect your existing practice, take time to address the following issues:

- Are employees responsible for equipping personal devices with software needed for work tasks?
- Who maintains the personal device hardware and software – the employee or the IT department?
- How will personal devices be linked to the nonprofit's network while minimizing the spread of malicious software (malware) and viruses?
- Will employees consent to IT staff having access to personal devices?

Erin Gloeckner is Project Manager at the Nonprofit Risk Management Center. Erin welcomes your feedback and questions about any of the topics addressed in this article at Erin@nonprofitrisk.org or (202) 785-3891.

Tech Risk Q & A

By Melanie Herman & Erin Gloeckner

Q: *What questions should we ask the references of a prospective new tech vendor?*

A: Checking references for any new vendor is a good idea and sound risk management practice. When checking references for a new technology vendor, try to ask questions that will enable you to get a sense of the quality and responsiveness you're likely to experience as a customer. If possible, ask for two current client references and at least one former client reference. Here are some questions to help you get started:

- Did the vendor honor the contract and warranties?
- Have you had any disputes (e.g., about contract terms and conditions, quality of service, etc.) with the vendor? If so, how were they handled?
- How would you rate the vendor's technical capabilities?
- How many people at the vendor do you work/interact with? Is customer service consistent or spotty?
- Has your nonprofit experienced any tech challenges or downside risks (e.g., data breaches) that required the tech vendor's responsive action? If yes, did the vendor respond in a timely fashion and was it able to resolve the problem you experienced?
- Would you recommend the vendor to other organizations? Why?
- What do you wish you had known before you started working with the vendor?

Q: *I'm concerned that some of our staff are spending up to four hours each day posting photos and material to their personal Facebook pages. What action should I take, if any?*

A: Virtually every nonprofit employee spends some time during the workday on personal matters, such as making medical appointments, answering calls from children, parents, caregivers and schools, and checking personal email or perusing social media accounts. Yet most employees understand that these tasks should constitute a small portion of the workday. As a result, most employers do not place strict time limits on such activities. However, when personal tasks and activity consume more than a fragment of an employee's paid work time, there are a number of potential negative consequences, including:

- Frustration or anger by co-workers who observe policy abuses;
- Organizational culture that places little value in HR rules and policies;
- Decline in productivity impairing the ability of the nonprofit to achieve its goals;
- Exposure of the nonprofit's tech resources to viruses, malware or other threats introduced by personal use of organization resources.

There are two general approaches to address the abuse of your existing "acceptable use" policy that asks employees to limit time spent during the workday on personal matters. The first approach is to rework the policy to include specific examples of acceptable and unacceptable uses of the nonprofit's systems, and provide training to the full team on the language and intent of the policy.

continued on next page

The second approach is to enforce your existing policy by addressing misuse with policy violators. Meet with any staff who are violating the policy and reiterate the negative consequences of policy abuse. Explain clearly what the staff member must do (or not do) to demonstrate compliance with the nonprofit's policies, and a timeframe for doing so. Clearly state the consequences of continued policy abuse.

Q: *What are the three most important considerations in selecting a Cloud storage vendor?*

A: A primary consideration is that the vendor meets your technical requirements. Do you understand your storage needs and existing IT infrastructure? If not, talk to your internal IT wizard or get help from an outside expert. Once you understand the scope of services you need, you will be in the best possible position to identify and then compare suitable vendors.

A secondary consideration is to select a vendor with a good reputation in the market. Hype surrounds the cloud and a vendor's capacity may not meet your expectations. Before entering a contract with a vendor, validate their claims. Request references from current and former clients and ask the vendor's clients if their expectations were met.

Another consideration is to request training and guidance from your candidates for cloud services. Require a training package with your contract, particularly if you don't have an IT expert on staff. Keep in mind that any cloud services you purchase should integrate seamlessly with other IT operations. One of your goals should be to find a vendor/partner who will empower your staff to use cloud services to achieve maximum benefit.

Q: *What are the risks, if any, of using donated PCs for our staff (from different sources) rather than buying or leasing new machines?*

A: One of the risks of using donated computers is that it may be hard to predict the total cost and time required to maintain these machines in working order. Before accepting donated computers, establish guidelines for determining which donations are suitable. Here are a few questions to resolve before you invite stakeholders to donate equipment to your nonprofit:

- Is your nonprofit able to accept both PCs and Apple products, or does it make sense to use only one or the other?
- What are your minimum requirements for any donated machine? If service delivery is dependent on every staff member being able to access custom case management software, make certain that you understand and document those minimum requirements.
- Do you have the resources to "clean" a donated computer of data and programs that you don't need?

Q: *Where can I find information about which insurers offer Cyber Liability policies?*

A: Consider searching for insurance providers using online insurance directories like www.kirschners.com. Remember that liability for loss of client or employee data is not typically covered in standard insurance policies. As discussed in the article titled *Insurance for Cyber Risks*, in most cases you'll need a cyber liability policy to protect against data breaches and other information age risks.

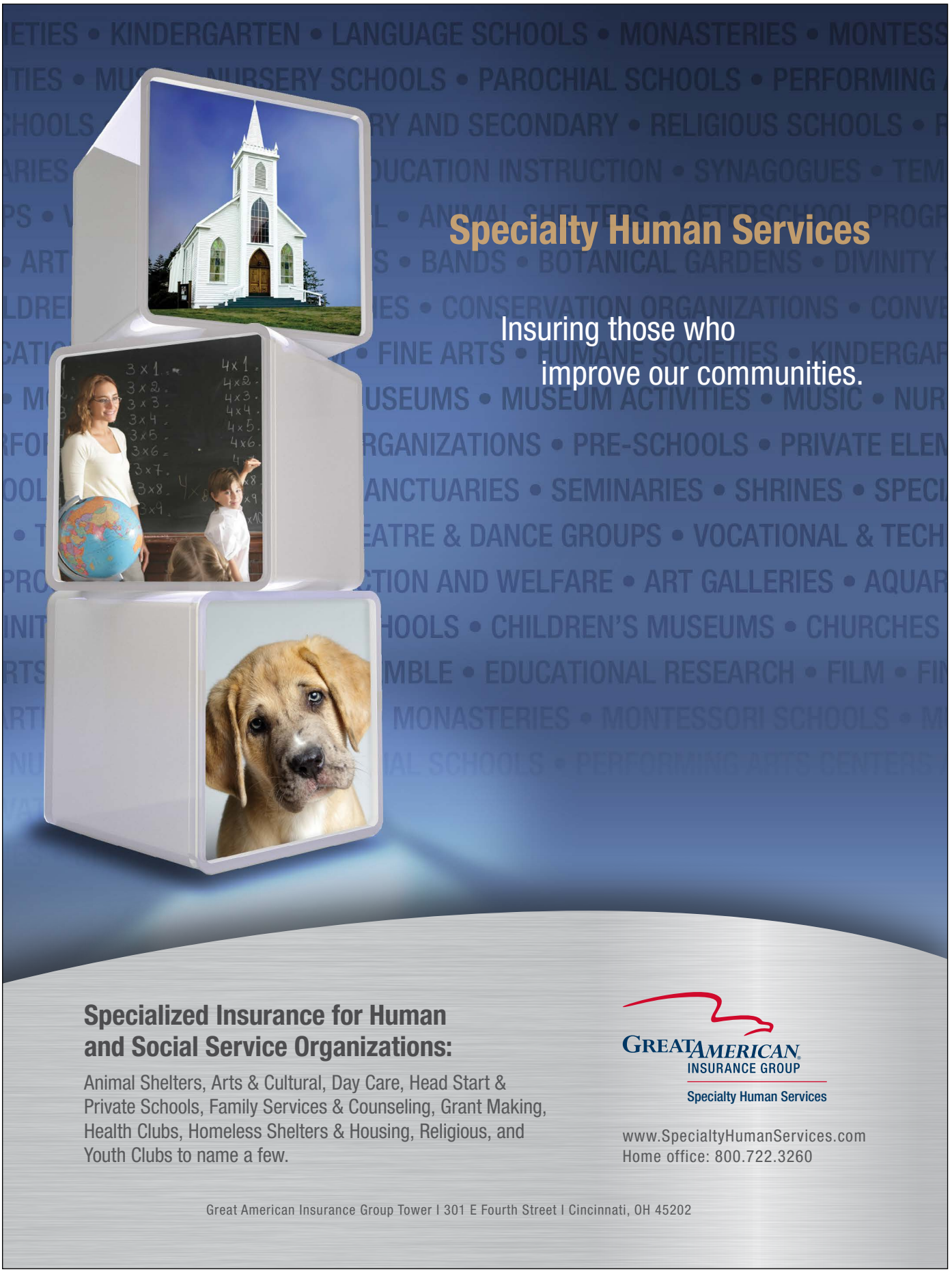
Q: *What are the first steps we should take if we become aware that personal donor information has been compromised?*

A: When your nonprofit experiences a data breach, PCI, HIPAA, and your state's regulatory requirements will dictate what you must do. Aim to understand your requirements long before this type of risk event occurs. Check in with your nonprofit's staff, contract or volunteer general counsel, tech vendor, and other partner advisers to develop a clear plan you can follow that will ensure a legally compliant response to the crisis. After the breach occurs and you have taken the necessary immediate steps, invite a third party firm to investigate if your IT department does not have the capacity to do so. For example, you may want to engage a computer forensic investigator or information security specialist. Keep in mind that you may be required to notify partners, customers, and/or government agencies about the breach; if possible, prepare draft crisis communication materials before the event. Finalize and disseminate your materials as soon as the breach occurs. You may also need to engage a credit monitoring firm to provide assistance to those who have been affected by the breach.

Erin Gloeckner is Project Manager at the Nonprofit Risk Management Center. Erin welcomes your feedback and questions about any of the topics addressed in this article at Erin@nonprofitrisk.org or (202) 785-3891.

Melanie Lockwood Herman is Executive Director of the Nonprofit Risk Management Center. She welcomes your feedback on this article and questions about the Center's resources at Melanie@nonprofitrisk.org or (202) 785-3891.

RISK MANAGEMENT MARKETPLACE



Inclusion in the Marketplace does not constitute an endorsement by the Nonprofit Risk Management Center. To inquire about space availability, contact Jennifer@nonprofitrisk.org.

Exclusively for 501(c)(3)s

More Than 2,000 Nonprofits Have Used Their *Unemployment Tax Exemption* to Save Thousands.

Find Out How.

Visit **www.ChooseUST.org** today.
Or call 1-888-249-4788 for a free savings evaluation.

UST
Save Money. Build Assets.

RISK MANAGEMENT MARKETPLACE

Nonprofit Risk Management Center

For rates & advertising availability, email jennifer@nonprofitrisk.org.

For our media kit, go to:
www.nonprofitrisk.org/Marketplace/advertise.asp

AH&T
INSURANCE

Specializing in insurance & risk management solutions for nonprofit organizations.

Rated the #1 firm for Directors & Officers insurance for nonprofit organizations by the *Tillinghast Survey*.

Mel Whiteley
20 South King Street
Leesburg, VA 20175
Phone: (703) 737-2212
Fax: (703) 771-1852
www.ahtins.com/nonprofits

RISK MANAGEMENT MARKETPLACE

Sports Leagues. One of over 100 specialty niches.

Where sports teams turn when they can't afford to lose.

At Philadelphia Insurance Companies, we specialize in servicing over 100 niche industries. Leading organizations in the world of sports, education, human services and many others turn to the experts at PHLY for our ability to write complex coverages at competitive rates. PHLY customers can feel secure knowing we have industry-leading customer service, are rated A++ by A.M. Best, and have a 97.5% claims satisfaction level. When you can't afford any gaps in your coverage, you can't afford to go with anyone but PHLY.

855.411.0796 | **PHLY.com/sports**

Download our free whitepaper
10 REASONS WHY YOU NEED SPECIALTY INSURANCE.

PHILADELPHIA INSURANCE COMPANIES
A Member of the Tokio Marine Group
Focus on the Things that Matter, We'll Handle the Risk!®

Philadelphia Insurance Companies is the marketing name for the property casualty insurance operations of Philadelphia Consolidated Holding Corp., a member of the Tokio Marine Group. All products are written by insurance company subsidiaries of Philadelphia Consolidated Holding Corp. Coverages are subject to actual policy language.

Inclusion in the Marketplace does not constitute an endorsement by the Nonprofit Risk Management Center. To inquire about space availability, contact Jennifer@nonprofitrisk.org.

Products/Publications/eBooks Order Form

	Price	No.	Total
PRODUCTS—ORDER ONLINE			
My Risk Management Policies at www.MyRiskManagementPolicies.org	$179.00		
My Risk Management Plan at www.MyRiskManagementPlan.org	$139.00		
BOOKS			
No Surprises: Harmonizing Risk and Reward in Volunteer Management—*5th Edition*	$25.00		
A Golden Opportunity: Managing the Risks of Service to Seniors	$ 8.00		
Coverage, Claims & Consequences: An Insurance Handbook for Nonprofits—*2nd Edition*	$30.00		
Managing Facility Risk: 10 Steps to Safety	$15.00		
More Than a Matter of Trust: Managing the Risks of Mentoring	$15.00		
The Season of Hope: A Risk Management Guide for Youth-Serving Nonprofits	$20.00		
Vital Signs: Anticipating, Preventing and Surviving a Crisis in a Nonprofit	$10.00		
eBOOKS			
Managing Special Event Risks: 10 Steps to Safety—*2nd Edition* (eBook only)	$20.00		
EXPOSED: A Legal Field Guide for Nonprofit Executives (eBook only)	$25.00		
Financial Risk Management: A Guide for Nonprofit Executives (eBook only)	$25.00		
Pillars of Accountability: A Risk Management Guide for Nonprofit Boards—*2nd Edition* (eBook only)	$12.00		
Ready...or Not: A Risk Management Guide for Nonprofit Executives—*2nd Edition* (eBook only)	$25.00		
Staff Screening Tool Kit—*3rd Edition* (eBook only)	$30.00		
Taking the High Road: A Guide to Effective & Legal Employment Practices for Nonprofits—*2nd Edition* (eBook only)	$45.00		
Playing to Win: A Risk Management Guide for Nonprofit Sports & Recreation Programs (eBook only)	$20.00		
		SUBTOTAL	
		Shipping & Handling	
		TOTAL	

Visit **www.nonprofitrisk.org/store/catalog.asp** for a complete description of all current titles, including tables of contents. All titles are available as eBooks—download our current titles and save shipping and handling costs.

Customer Information

NAME _____ TITLE _____

ORGANIZATION _____

ADDRESS _____

CITY _____ STATE _____ ZIP _____

TEL _____ FAX _____

E-MAIL _____

Method of Payment

❑ Check enclosed ❑ P.O. # _____ Charge my: ❑ Visa ❑ MasterCard ❑ AmEx

CARD NO _____ EXP. DATE _____ VERIFICATION CODE (FOR MC/VISA 3 DIGIT ON THE BACK, AMEX 4 DIGIT ON THE FRONT)

SIGNATURE _____

Order online at www.nonprofitrisk.org
Call (202) 785-3891 to inquire about quantity discounts.

Shipping & Handling

Please add $4.00 for each book ordered. For example, if you order two books the shipping & handling cost is $8.00.

Mail or fax this form with payment to:

Nonprofit Risk Management Center

15 N. King St., Suite 203, Leesburg, VA 20176
Telephone: (202) 785-3891 • Fax: (703) 443-1990

Nonprofit
Risk Management
Center

15 N. King St., Suite 203
Leesburg, VA 20176

Risk Management ESSENTIALS

Tips, Knowledge and Tools for Nonprofit Organizations

Affiliate Members:

- Access National Bank
- Adventist Risk Management, Inc.
- ANCOR (American Network of Community Options and Resources)
- Career Opportunities Development, Inc.
- CGSHB
- Communities In Schools
- Community Action Partnership
- Council Services Plus, Inc.
- EarthCorps
- Frisco Family Services
- Girl Scouts of Greater Atlanta, Inc.
- Gulf Coast Community Foundation
- Gulf Coast Social Services
- Harleysville Insurance
- Hays Affinity
- Hillel: The Foundation for Jewish Campus Life
- HMS School for Children with Cerebral Palsy
- Housing Authority Insurance Group, Inc.
- John Gear Law Office, LLC
- Kentucky Nonprofit Network
- Kingsley House, Inc.
- Loudoun Human Services Network
- Maine Association of Nonprofits
- Maryland Nonprofits
- Metropolitan Arts Partnership
- Michigan Nonprofit Association
- N.C. Center for Nonprofits
- National MS Society
- NeighborWorks America
- Nunavut Literacy Council
- OCCK, Inc.
- Pennsylvania Association of Nonprofits Organizations
- PSA Insurance & Financial Services
- Rebuilding Together
- Speech and Language Development Center
- State Bank Financial
- Sunshine
- Texas Association of Nonprofit Organizations
- The Ford Family Foundation
- The Miller Group
- TransitionGuides, Inc.
- United Way Worldwide
- US Olympic Committee
- YMCA of the USA

Inside This Issue

Please route to:

☐ Executive Director ☐ Director of Volunteers ☐ Risk Manager
☐ Legal Counsel ☐ Human Resources ☐ Finance/Administration