سوالات فوق نوع ملاحظات امنیتی را که می توانند در مبادلات تجارت الکترونیکی مطرح باشند، بیان می نمایند. برای مبادلاتی که شامل پرداخت الکترونیکی می شوند، می بایست ملاحظات امنیتی دیگری را نیز در نظر گرفت. بزرگترین ملاحظات امنیتی تجارت الکترونیکی عبارتند از:

الف- اعتبار سنجی (Authentication): فرآیندی که هویت اشخاص و سازمان ها را در اینترنت تأیید و تصدیق می کند.

ب- اختیاردهی (Authorization): فرآیندی که با بررسی صلاحیت افراد، به آنها اجازه دسترسی به منابع ذکر شده را می دهد.

پ-بازرسی (Auditing): هر اطلاعات و پایگاه داده هایی که افراد در وب سایت دیدن کرده، یا به آنها دسترسی پیدا می کنند، بازرسی نامیده می شود. بازرسی به پرسنل فناوری اطلاعات سازمان این اجازه را می دهد تا حتی افراد بازدید کننده از وب سایت را شناسایی کنند.

ت-قابلیت اعتماد (Confidentiality): حریم خصوصی (Privacy): اطلاعات خصوصی و محرمانه افراد نباید برای افراد فاقد مجوز و نیز نرم افزارهای کامپیوتری فاش شود.

ث- یکپارچگی (Integrity): اطلاعات ممکن است هنگام انتقال یا بعد از ذخیره شدن، به سرقت رفته یا خراب شوند. به قابلیت حفاظت از اطلاعات برای جلوگیری از به سرقت رفتن آنها، اصطلاحاً یکپارچگی گفته می شود.

ج- قابلیت دسترسی (Availability): به وب سایتی در دسترس می گویند که کاربران بتوانند در هر زمان که می خواهند، به صفحات، اطلاعات یا خدمات آن دسترسی پیدا کنند.

چ-عدم انکار (Non repudiation): فرآیندی است که قابلیت هر گونه امتناع کاربر در عدم انجام سفارش را از او می گیرد. یکی از تکنیک های کلیدی در عدم انکار، امضاء الکترونیکی (Electronic Signature) می باشد.

۷-۳- انواع تهدیدات و تهاجمات امنیتی در تجارت الکترونیکی

دو روش عمده برای تهدیدات امنیتی در تجارت الکترونیکی وجود دارد که شامل فنی و غیر فنی می شوند.

دو روش غیر فنی، با استفاده از ضد و نقیض گویی و فریب کاربران، آنها را وادار می کنند تا اطلاعات شخصی خود را فاش سازند. به تهدیدات غیر فنی اصطلاحاً مهندسی اجتماعی (Social Engineering) می گویند.

در مقابل، استفاده از نرم افزارها و سیستم های مختلف برای دستیابی به اطلاعات کاربران را تهدیدات فنی می گویند. ویروس های کامپیوتری نمونه ای از تهدیدات فنی تجارت الکترونیکی هستند.

۷-۳-۱- تهدیدات غیر فنی تجارت الکترونیکی

دو دسته تهدیدات غیر فنی وجود دارند که شامل انسان مدار و کامپیوتر مدار می شوند.

تهدیدات غیر فنی انسان مدار، بر پایه روش های سنتی ارتباطات (مانند تلفن) استوار است. (جا زدن هکر بجای پرسنل IT سازمان) تهدیدات غیر فنی کامپیوتر مدار بر پایه روش هایی مانند ارسال پست الکترونیکی استوار است.

سه راهکار زیر برای مقابله با تهدیدات غیر فنی تجارت الکترونیک توصیه شده است:

الف- آموزش و یادگیری ب- سیاست ها و روش ها ج- آزمایش سازمان از لحاظ امنیتی

۷-۳-۲- تهدیدات فنی تجارت الکترونیکی

تهدیدات فنی تجارت الکترونیکی بیشتر بر پایه نرم افزارها و سیستم های دانش مدار استوار است. روش های متفاوتی برای تهدیدات فنی کاربران وجود دارد. با جستجو در اینترنت می توان به راحتی به نرم افزارهای قدرتمندی دست یافت که بعضاً رایگان در اختیار کاربران قرار می گیرند و این امکان را برای آنها فراهم می سازند تا به نقاط آسیب پذیر سیستم مورد نظر دست یابند.

۷-۳-۳- ویروس ها، کرم ها و تروجان های اینترنتی

الف- ویروس ها: یکی از معروفترین عواملی هستند که منجر به آلوده شدن کاربران می شوند.

ویروس ها کدهای نرم افزاری هستند که وارد کامپیوتر کاربر شده، سیستم عامل آنرا در حد آنچه برایش تعریف شده، در اختیار می گیرد. البته ویروس ها خودبخود فعال نمی شوند و لازم است که کاربر خود آنرا فعال کند. همچنین ویروس ها توانایی تکثیر خودکار از یک کامپیوتر به کامپیوتر دیگر را ندارند و به یک کاربر برای فعال شدن نیاز دارند.

ب- کرم ها: بزرگترین تفاوت بین ویروس ها و کرم ها در این است که کرم ها در سیستم ها و بخصوص شبکه ها براحتی منتقل می شوند اما ویروس ها تنها جنبه محلی دارند و بدون اجازه کاربر قابل انتقال نیستند.

کرم ها برنامه های کامپیوتری هستند که بصورت مستقل اجرا شده، فعالیت سیستم عامل کاربر را ر اختیار می گیرند. همچنین آنها نسخه ای کامل از خود را از طریق شبکه بصورت خودکار به سیستم های دیگر منتقل می کنند.

پ-تروجان ها: تروجان ها برنامه هایی هستند که در ظاهر مفید و قابل استفاده اند، اما محتوای بسیار خطرناکی دارند و برای امنیت سیستم، ریسک بزرگی محسوب می شوند.

۷-۴- مدیریت امنیت تجارت الکترونیک

اگرچه آگاهی از موارد امنیتی در سال های اخیر افزایش یافته است، با اینحال سازمان ها همچنان اشتباهات زیر را در زمینه مدیریت امنیت مرتکب می شوند:

a. **نداشتن ارزش واقعی اطلاعات:** سازمان های بسیار کمی وجود دارند که ارزش واقعی دارایی های اطلاعاتی خود را بدانند.

b. **تعریف نادرست مرزهای امنیتی:** بیشتر سازمان ها تنها به حفاظت امنیتی از شبکه های داخلی خود می پردازند و چندان توجهی به امنیت شرکای زنجیره تأمین خود ندارند.

c. **مدیریت امنیت انفعالی:** سازمان ها تنها زمانی به امنیت توجه می کنند که دچار مشکلات خاص آن شوند.

d. **به روز نشدن فرآیندهای مدیریت امنیت:** سازمان ها بسیار به ندرت اقدام به تغییر و بروز کردن موارد امنیتی خود می کنند.

e. **دید سطحی/ بخشی نسبت به امنیت:** امنیت عموماً به چشم یک مشکل، تنها برای واحد IT دیده می شود نه به چشم یک مشکل برای کل سازمان.

برای بررسی بیشتر مدیریت امنیت اطلاعات، باید سه فاز اصلی مدیریت بحران های امنیتی به شرح زیر پرداخته شود:

الف- شناسایی دارایی ها: سازمان می بایست کامپیوترهای کلیدی، شبکه و سرمایه های اطلاعاتی خود را شناخته، برای آنها ارزش گذاری نماید.

ب- ارزیابی ریسک: پس از ارزش گذاری دارایی ها، می بایست به شناسایی مواردی که بعنوان تهدید برای دارایی های کلیدی سازمان به حساب می آیند، پرداخت.

پ-پیاده سازی: پس از شناسایی ریسک های اصلی سازمان، می بایست لیستی از راه حل ها برای ریسک های با اولویت بالا در نظر گرفته شوند. همچنین این راه حل ها باید بر اساس تحلیل سود- هزینه کلی ارزیابی شوند.

۷-۵- موضوعات اخلاقی

اخلاق، شاخه ای از فلسفه است که به بحث در مورد کارهای درست و نادرست می پردازد.

در طول سالیان متمادی، فلاسفه خطوط راهنمای اخلاقی بسیاری را ارئه کرده اند، اما همچنان نمی توان گفت هر عمل غیر اخلاقی، لزوماً غیر قانونی نیز هست. در محیط پیچیده امروز، همیشه تعاریف کارهای درست و نادرست، واضح نیستند. همچنین تفاوت های زیادی بین اخلاقی و غیر اخلاقی بودن کارها در فرهنگ کشورهای مختلف وجود دارد.

در یک بررسی، چارچوب موضوعات اخلاقی به شرح زیر بیان شده است:

الف- خصوصی: جمع آوری، ذخیره و توزیع اطلاعات درباره افراد

ب- صحت: اصالت، درستی و صحت اطلاعات جمع آوری شده و پردازش شده

پ- مالکیت: مالکیت و ارزش اطلاعات و مالکیت معنوی

ت- قابلیت دسترسی: حق دسترسی به اطلاعات و پرداخت هزینه برای دسترسی به آن

۷-۶-موضوعات قانونی

پیاده سازی تجارت الکترونیکی، موضوعات قانونی بسیاری را به همراه دارد، که می توان این موضوعات را در قالب های مختلفی به شرح زیر طبقه بندی کرد:

الف- خصوصی شدن اطلاعات: این موضوع، اهمیت فوق العاده ای برای مشتریان دارد. مشتریان عموماً تمایل ندارند اطلاعات شخصی شان را دیگران (مشخصات فردی و اینکه چگونه و چه چیزهایی را می خرند) بدانند.

ب-مالکیت معنوی (Copy Right): کپی برداری و توزیع اطلاعات الکترونیکی آسان و ارزان است و به همین دلیل محافظت از مالکیت معنوی آنها بسیار دشوارتر است.

پ-گفتگوی آزاد (Free Speech): اینترنت، بزرگترین بستر برای گفتگوی آزاد را فراهم می سازد. با این حال، این آزادی ممکن است بعضی افراد را آزار دهد یا در تضاد با قانون مبارزه با ابتذال فرهنگی باشد.

ت- محافظت از مصرف کننده: بسیاری از موضوعات غیر قانونی در رابطه با محافظت از مصرف کننده، از جمله ارائه نامناسب و بدون کیفیت محصولات یا خدمات و ... در تجارت الکترونیکی دیده می شود.

ث- سایر موضوعات قانونی: سایر موضوعات قانونی در رابطه با تجارت الکترونیکی شامل اعتبار قراردادها، داوری و قضاوت در تجارت ها، قماربازی، سیاست های رمزگذاری و ... در اینترنت می شوند.

۷-۷-موضوعات قانونی در مقایسه با موضوعات اخلاقی

موضوعات قانونی و اخلاقی، در موفقیت تجارت الکترونیکی، نقش مهمی ایفا می کنند.

در تئوری می توان بین موضوعات قانونی و اخلاقی تفاوت قائل شد. اگر شما کار غیر قانونی انجام دهید، قانون را زیر پا گذاشته اید. اگر کار غیر اخلاقی انجام دهید، ممکن است کاری غیر قانونی تلقی نشود.

بطور وضوح، بسیاری از قوانین غیر قانونی، غیر اخلاقی هستند. در فناوری اطلاعات، تشخیص مسائل اخلاقی مشکل است.