چکیده

حرکت اخیر سازمان‌ها، خصوصاً سازمان‌های پولی- مالی به‌سمت جامعه اطلاعاتی و نقش مؤثر و تحول‌آفرین IT در این زمینه، باعث شده است بانک‌ها به‌عنوان یک نهاد مالی و اعتباری مهم در هر نظام اقتصادی برای بقای خود در عصر اطلاعات،استانداردسازی امنیت اطلاعات را برای اجرای مؤثر و مناسب جدی بگیرند.

بدیهی است رابطه میان سودآوری یک مؤسسه مالی و ریسک حاکم بر آن، یک رابطه تعیین‌کننده است. لذا سود یک بنگاه اقتصادی که از تعامل مستمر با مشتریانش به‌دست می‌آیند، موضوعی است که امروزه برای تمامی واحدهای اقتصادی تعیین‌کننده است، زیرا مشتریانی به‌سمت یک مؤسسه مالی و اعتباری روی می‌آورند که علاوه بر اطمینان بیشتر از اطلاعات و عملیات بانکی، سودآوری خود را نیز تضمین شده بدانند. از سوی دیگر افزایش کیفیت و کمیت خدمات بانکی، راهکاری برای جذب مشتریان بیشتر است. بانکداری الکترونیک نیز از جمله خدمات جدیدی است که در سال‌های اخیر بانک‌ها و مؤسسات پولی و مالی به آن روی آورده‌اند.

با عنایت به موضوعات بحث شده، بانکداری الکترونیک به‌عنوان درگاهی در فضای وب می‌تواند از طریق تبادل اطلاعات، تمام عملیات مالی و اعتباری مشتریان را با مؤسسات پولی و مالی انجام دهد. بانکداری الکترونیک در استانداردسازی و دستیابی به سطح مشخصی از امنیت همواره مورد تأکید مشتریان و ذینفعان مؤسسه پولی و مالی می‌باشد. در این مقاله سعی شده است با ورود به چگونگی ایجاد حفاظت‌های امنیتی شبکه در سطح الکترونیکی خدمات و فعالیت‌ها، استانداردهای مربوط به آن نیز مورد بررسی و تجزیه و تحلیل قرار گیرد.

کلمات کلیدی: امنیت اطلاعات، استانداردهای مرجع، ایمن‌سازی، ریسک، بانکداری الکترونیک.

۱- مقدمه

اطلاعات گنجینه‌ای که تا چندی قبل در کمدها و پستوهای بانک‌ها نگهداری می‌شد، از چندسال قبل و با توسعه شبکه‌های محلی درون بانکی، به شبکه داخلی بانک‌ها راه یافت. در آن زمان، اطلاعات محدود کاربران شبکه و اعمال کنترل‌های مدیریتی، محافظت‌های فیزیکی و محدود نمودن تعداد افرادی که به سرویس‌ها و به‌ویژه سرویس‌های حساس دسترسی داشتند، موجب می‌شد تا مشکل خاصی بروز نکند. اما اینک با اتصال شبکه‌های بانکی به شبکه جهانی، همان گنجینه حساس در معرض دید و استفاده طیف وسیعی از مخاطبین در سراسر جهان قرار گرفته است. به‌علاوه این‌که بانک یک مؤسسه مالی با تراکنش‌های مالی فراوان است که این تراکنش‌ها با حجم بانک و افزایش خدمات جدید بانکی که از ملزومات بقا در حوزه رقابتی بانک‌ها است، افزایش می‌یابد.

در این شرایط، تأمین امنیت همان گنجینه گرانمایه یعنی اطلاعات، بدون شک یکی از ضروریات هر بانکی است. حاصل تجربه و اقدامات انجام شده در طول دهه‌های گذشته در جهان، رویکردی است تحت‌عنوان سیستم مدیریت امنیت اطلاعات.

با ارائه اولین استاندارد مدیریت امنیت اطلاعات در سال ۱۹۹۵، نگرش سیستماتیک به مقوله امنیت اطلاعات شکل گرفت. براساس این نگرش، تأمین امنیت اطلاعات در یک مجموعه بانکی، به‌یکباره ممکن نیست و لازم است این امر به‌صورت مداوم و در یک چرخه ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح انجام گیرد. برای این منظور لازم است هر بانک بر اساس یک متدولوژی مشخص، ضمن تهیه طرح‌ها و برنامه‌های امنیتی مورد نیاز، تشکیلات لازم جهت ایجاد و تداوم امنیت اطلاعات خود را نیز ایجاد کند. در بخش‌های بعدی به مقوله امنیت اطلاعات با رویکرد بانکی می‌پردازیم.

۲- ضرورت و اهمیت امنیت اطلاعات و ایمن‌سازی کامپیوترها

تمامی رایانه‌ها از رایانه‌های موجود در منازل گرفته تا رایانه‌های موجود در بانک‌ها و مؤسسات بزرگ، در معرض آسیب و تهدیدهای امنیتی می‌باشند. با انجام تدابیر لازم و استفاده از برخی روش‌های ساده می‌توان پیشگیری لازم و اولیه‌ای را در خصوص ایمن‌سازی محیط کامپیوتری انجام داد. علیرغم تمامی مزایا و دستاوردهای اینترنت ، این شبکه عظیم به همراه فن‌آوری‌های مربوطه، دریچه‌ای را در مقابل تعداد زیادی از تهدیدهای امنیتی برای تمامی استفاده‌کنندگان (افراد، خانواده‌ها، بانک‌ها، مؤسسات و ...)، گشوده است. با توجه به

ماهیت حملات، می‌بایست در انتظار نتایج نامطلوب متفاوتی بود (از مشکلات و مزاحمت‌های اندک تا از کار انداختن سرویس‌ها و خدمات). در معرض آسیب قرارگرفتن داده‌ها و اطلاعات حساس، تجاوز به حریم خصوصی کاربران، استفاده از کامپیوتر کاربران برای تهاجم برعلیه سایر کامپیوترها، از جمله اهداف مهاجمانی است که با بهره‌گیری از آخرین فن‌آوری‌های موجود، حملات خود را سازماندهی می‌کنند. بنابراین، باید به موضوع امنیت اطلاعات، ایمن‌سازی کامپیوترها و شبکه‌های کامپیوتری، توجه جدی شده و از فرآیندهای متفاوتی در جهت مقاوم‌سازی آنان، استفاده شود.

با یک نگاه تاریخی، رویکرد مکانیزاسیون و نفوذ رایانه‌های شخصی در بانک‌های ایرانی به دهه ۱۳۶۰ شمسی بر می‌گردد[۱]، شاید تا آن زمان تردیدها و مقاومت‌ها در به‌کارگیری رایانه‌های شخصی و فرآیندهای مکانیزه به دلیل تبعات ناشی از ریسک عملیاتی و سوء استفاده‌های ناشی از محیط سایبر نبوده بلکه عامل مقاومت در عدم آشنائی با پدیده فناوری اطلاعات و عادت نمودن به فرآیندهای سنتی و اجرایی‌شدن تمامی فرآیندها به‌روش سنتی بوده است. اخیراً با گسترش بانکداری الکترونیک و ریسک پذیری بالای آن، حجم بالایی از مطالعات امنیتی یک سازمان را در بر می‌گیرد. ریسک عملیاتی بانکداری الکترونیک و ضرر و زیان ناشی از آن با گسترش و توسعه بانکداری الکترونیک اینترانتی و افزایش کانال‌های دیجیتالی بدون حضور و مراجعه مشتریان به شعبه نیز از اواخر دهۀ ۱۳۷۰ شمسی آغاز شده است. گسترش خدمات و محصولات بین بانکی از طریق شبکه شتاب و راه‌اندازی سیستم تسویه ناخالص آنی (RTGS)[۲] بین بانک‌ها از سوی بانک مرکزی و ارائه خدمات برداشت و انتقال وجوه از طریق دستگاه‌های PINPAD[۳]، EFT[۴] و POS[۵] برغم تمامی مزیت‌ها و رضایت مشتریان هنوز سابقه زیادی در بانکداری ایران ندارد و هنوز بسیاری از مسائل مربوط به ریسک و سیستم‌های نظارتی مکانیزه و مشکلات ناشی از آن برای برخی از بانک‌ها و مؤسسات مالی و مشتریان آشکار نشده است.

تبعات سوء ناشی از عدم وجود مدیریت ریسک مبتنی بر فناوری برای ردگیری تراکنش‌ها، مانیتور نمودن کانال‌های توزیع دیجیتال می‌تواند به افزایش هزینه‌های سربار بانک‌ها و

---

[۱] جهت اطلاعات بیشتر مراجعه شود به اللهیاری فرد، محمود، "خدمات بانکداری الکترونیک و نیازهای اجرایی آن در مقایسه تطبیقی خدمات مختلف بانکی"، پژوهشکده پولی و بانکی بانک مرکزی ج.ا.ا، ۱۳۸۴.

[2] Real Time Grass Settlement

[3] POSشعب

[4] Electronic Fund Transfer

[5] Point Of Sale

مؤسسات پولی و مالی منجر و یا حتی ممکن است ارائه خدمات مبتنی بر فناوری را با شکست روبرو کند.

وجود یک حفره و یا مشکل امنیتی، می‌تواند یک بانک یا مؤسسه پولی و مالی را به‌روش‌های متفاوتی تحت‌تأثیر قرار دهد. آشنایی با عواقب خطرناک یک حفره امنیتی در یک مؤسسه پولی و مالی و شناسایی مهم‌ترین تهدیدات امنیتی که می‌تواند حیات یک مؤسسه پولی و مالی را با مشکل مواجه کند، از جمله موارد ضروری به‌منظور طراحی و پیاده‌سازی یک مدل امنیتی در یک مؤسسه پولی و مالی است.

وجود حفره‌های امنیتی در یک مؤسسه پولی و مالی، می‌تواند پیامدهای منفی متعددی به‌دنبال داشته باشد که عبارتند از:

- کاهش درآمد و افزایش هزینه
- خدشه به اعتبار و شهرت یک مؤسسه پولی و مالی
- از دست دادن داده و اطلاعات مهم
- اختلال در فرآیندهای جاری یک مؤسسه پولی و مالی
- پیامدهای قانونی به‌دلیل عدم ایجاد یک سیستم ایمن و تأثیر جانبی منفی بر فعالیت سایر مؤسسات پولی و مالی
- سلب اعتماد مشتریان
- سلب اعتماد سرمایه گذاران

که هر یک از موارد فوق ریسک‌های مربوط به خود را به همراه خواهد داشت.

۳- تاریخچه استانداردسازی امنیت اطلاعات

هر بانک یا مؤسسه مالی و اعتباری می‌باید یک چارچوب و یا framework امنیتی فعال و پویا برای خود ایجاد و به‌درستی از آن نگهداری کند. دو استاندارد BS7799 و ISO/IEC TR 13335 به‌عنوان منابعی برای برقراری امنیت در بانک‌ها و مؤسسات پولی و مالی مورد استفاده قرار می‌گیرند، که همه جوانب امنیّتی را تأمین می‌کنند.

منشاء استاندارد British Standard BS7799 به‌زمان تأسیس مرکز Commercial Computer Security Center و شکل‌گیری بخش DTI[1] در سال ۱۹۸۷ بر می‌گردد. این مرکز به‌منظور تحقق دو هدف تشکیل شد. اول تعریف معیارهایی بین‌المللی برای ارزیابی میزان

[1] UK Department of Trade and Industry

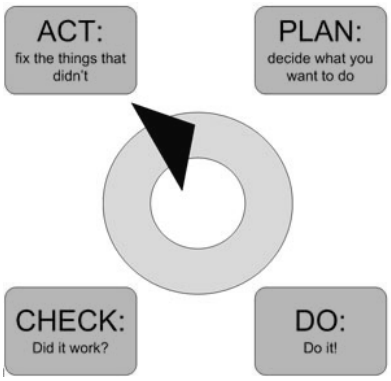
امنیت تجهیزات تولید شده توسط سازندگان تجهیزات امنیتی، به‌منظور ارائه تأییدیه‌های مربوطه و دوم کمک به کاربران.

برای این منظور، مرکز CCSC در سال ۱۹۸۹ اقدام به انتشار کدهایی برای سنجش میزان امنیت کرد که به "Users Code of Practice" معروف شد. چندی بعد، اجرایی‌بودن این کدها از دیدگاه کاربر، توسط مرکز محاسبات بین‌المللی NCC و یک کنسرسیوم از کاربران که به‌طورکلی از صاحبان صنایع در انگلستان بودند مورد بررسی قرار گرفت. اولین نسخه این استاندارد به‌عنوان مستندات راهبری PD ۰۰۰۳ در انگلستان منتشر شد. در سال ۱۹۹۵ این استاندارد با عنوان BS7799 منتشرشد و قسمت دوم آن نیز در فوریه سال ۱۹۹۸ به آن اضافه گردید. این قسمت مفهوم سیستم مدیریت امنیت اطلاعات ISMS[1] به‌وجود آورد. این سیستم ISMS به مدیران این امکان را می‌دهد تا بتوانند امنیت سیستم‌های خود را با حداقل نمودن ریسک‌های تجاری کنترل کنند. نسخه بازنگری شده این استاندارد در سال ۱۹۹۵ به‌عنوان استاندارد ISO ثبت گردید. در مجمعی که رأی موافق به ثبت این استاندارد به‌عنوان استاندارد ISO داده بودند، کشورهایی نظیر استرالیا و نیوزلند با اندکی تغییر، آن را در کشور خود با عنوان AS/NZS4444 منتشر کردند. طی سال‌های ۱۹۹۹ تا ۲۰۰۲ بازنگری‌های زیادی روی این استاندارد صورت گرفت. در سال ۲۰۰۰ با افزودن الحاقیه‌هایی به استاندارد BS7799 که به‌عنوان یک استاندارد ISO ثبت شده بود، این استاندارد تحت عنوان استاندارد ISO/IEC17799 به‌ثبت رسید.

نسخه جدید و قسمت دوم این استاندارد در سال ۲۰۰۲ به‌منظور ایجاد هماهنگی بین این استاندارد مدیریتی و سایر استانداردهای مدیریتی نظیر ISO ۹۰۰۱ و ISO ۱۴۰۰۱ تدوین شد. این قسمت برای ارزیابی میزان مؤثربودن سیستم ISMS در یک سازمان مدل PDCA[2] را همان‌گونه‌که در شکل (۱) نشان داده شده است ارائه می‌نماید.

[1] Information Security Management System
[2] Plan-Do-Check-Act

شکل ۱: مدل PDCA



ذیلاً به توضیحی راجع به استاندارد BS7799 می‌پردازیم.

استاندارد BS7799 اولین استاندارد مدیریت امنیت اطلاعات است که توسط مؤسسه استاندارد انگلیس ارائه شده است. نسخه اول این استاندارد (BS7799:1) در سال ۱۹۹۵ و در یک بخش منتشر شد و نسخه دوم آن (BS7799:2) که در سال ۱۹۹۹ ارائه و علاوه بر تغییر نسبت به نسخه اول، در دو بخش مستقل ارائه شد. همچنین آخرین نسخه این استاندارد، (BS7799:2002) در سال ۲۰۰۲ و همانند نسخه دوم، در دو بخش انتشار یافت. این استاندارد در حال حاضر به‌صورت فراگیر در سطح جهان مورد استفاده قرار می‌گیرد و بر اساس آمار منتشر شده در سایت گروه کاربران بین‌المللی سیستم مدیریت امنیت اطلاعات (ISMS IUG)[1] تا آوریل سال ۲۰۰۷ مجموعاً تعداد ۳۵۴۰ مؤسسه پولی و مالی در سطح جهان، موفق به اجرای ISMS براساس این استاندارد و اخذ تأییدیه از مراکز صدور گواهی مبتنی بر این استاندارد شده‌اند. جزئیات در جدول (۱) دیده می‌شود.

۴- استانداردهای مدیریت امنیت اطلاعات

در حال حاضر مجموعه‌ای از استانداردهای مدیریتی و فنی امنیت اطلاعات و ارتباطات، ارائه شده‌اند که استاندارد مدیریتی BS7799 مؤسسه استاندارد انگلیس، استاندارد مدیریتی ISO/IEC17799 و گزارش فنی ISO/IEC TR13335 مؤسسه بین‌المللی استاندارد، از برجسته‌ترین

[1] Information Security Management System International User Group

استانداردها و راهنماهای فنی محسوب می‌شوند. در این استانداردها، نکات زیر مورد توجه قـرار گرفته است:

- تعیین مراحل ایمن‌سازی و نحوه شکل‌گیری چرخه امنیت.
- جزئیات مراحل ایمن‌سازی و تکنیک‌های فنی مورد استفاده در هر مرحله.
- فهرست و محتوای طرح‌ها و برنامه‌های امنیت اطلاعات مورد نیاز مؤسسه پولی و مالی.
- ضرورت و جزئیات ایجاد تشکیلات سیاستگذاری، اجرایی و فنی تأمین امنیت.
- کنترل‌های امنیتی مورد نیاز برای هر یک از سیستم‌های اطلاعاتی و ارتباطی.

جدول۱: آمار اعضای استاندارد امنیت اطلاعات

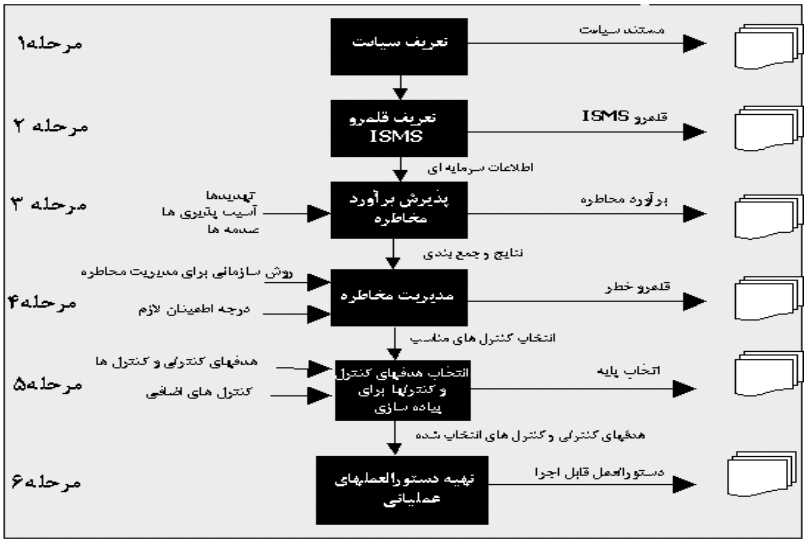
Japan	۲۰۴۳*	Austria	۱۱	Oman	۲
UK	۳۲۹	Saudi Arabia	۹	Pakistan	۲
India	۲۸۵	Spain	۹	Slovak Republic	۲
Taiwan	۱۲۷	Philippines	۸	South Africa	۲
Germany	۷۴	Sweden	۸	Sri Lanka	۲
Hungary	۵۷	UAE	۸	Armenia	۱
Korea	۴۹	Iceland	۷	Bulgaria	۱
USA	۴۸	Greece	۵	Gibraltar	۱
China	۴۷	Kuwait	۵	Egypt	۱
Italy	۴۳	Russian Federation	۵	Lebanon	۱
Australia	۴۲	Thailand	۴	Lithuania	۱
Netherlands	۳۱	Argentina	۳	Luxemburg	۱
Singapore	۲۸	Bahrain	۳	Macedonia	۱
Hong Kong	۲۶	Canada	۳	Moldova	۱
Czech Republic	۲۵	Croatia	۳	Morocco	۱
Malaysia	۱۹	France	۳	New Zealand	۱
Poland	۱۷	Indonesia	۳	Peru	۱
Brazil	۱۵	Isle of Man	۳	Qatar	۱
Ireland	۱۵	Macau	۳	Serbia and Montenegro	۱
Switzerland	۱۵	Romania	۳	Ukraine	۱
Finland	۱۴	Slovenia	۳	Uruguay	۱
Norway	۱۴	Belgium	۲	Vietnam	۱
Turkey	۱۳	Colombia	۲	Relative Total	۳۵۴۰
Mexico	۱۲	Denmark	۲	Absolute Total	۳۵۳۰*

۱-۴- بخش اول استاندارد BS7799:2 1999

در بخش اول این استاندارد، که تحت عنوان "آیین‌نامه کار مدیریت امنیت اطلاعات" ارائه شده است، مجموعه کنترل‌های امنیتی مورد نیاز سیستم‌های اطلاعاتی و ارتباطی هر مؤسسه پولی و مالی، در قالب ده دسته‌بندی کلی شامل موارد زیر، ارائه شده است:

۱- تدوین سیاست امنیتی مؤسسه پولی و مالی
۲- تشکیلات امنیتی
۳- طبقه‌بندی سرمایه‌ها و تبیین کنترل‌های لازم
۴- امنیت پرسنلی
۵- امنیت فیزیکی و پیرامونی
۶- مدیریت ارتباطات و بهره‌برداری
۷- کنترل دسترسی
۸- توسعه و پشتیبانی سیستم‌ها
۹- مدیریت تداوم فعالیت
۱۰- سازگاری

شکل۲: ایجاد چارچوب مدیریت امنیت اطلاعات



۲-۲-۴- بخش دوم استاندارد BS7799:2 1999

در این بخش از استاندارد که تحت عنوان "ویژگی‌های سیستم مدیریت امنیت اطلاعات" ارائه شده است، ضمن تأکید بر ضرورت ایجاد سیستم مدیریت امنیت اطلاعات، نیازهای سیستم مدیریت امنیت اطلاعات و کنترل‌های همه‌جانبه که برای تأمین امنیت اطلاعات، مورد نیاز می‌باشند، ارائه شده است.

۱- نیازهای سیستم مدیریت امنیت اطلاعات: در این قسمت تأکید شده که هر مؤسسه پولی و مالی، باید سیستم مدیریت امنیت اطلاعات خود را مستند، تعریف، ایجاد و نگهداری کند. در چارچوب مدیریتی ارائه شده در این بخش از استاندارد که در شکل (۲) ارائه شده است، لازم است مراحل شش‌گانه زیر برای مدیریت امنیت اطلاعات در نظر گرفته شوند:

- تعریف سیاست امنیت اطلاعات.
- تعریف قلمرو سیستم مدیریت امنیت اطلاعات و مرزبندی آن، متناسب با نوع و نیازهای مؤسسه پولی و مالی.
- انجام و پذیرش برآورد مخاطرات، متناسب با نوع و نیازهای مؤسسه پولی و مالی.
- پیش‌بینی زمینه‌ها و نوع مخاطرات، بر اساس سیاست‌های امنیتی.
- انتخاب هدف‌های کنترل و کنترل‌های مناسب که قابل توجیه باشند، از فهرست کنترل‌های همه جانبه.
- تدوین دستورالعمل‌های عملیاتی.

۲- کنترل‌های همه جانبه.

۵- مرجع پیاده‌سازی سیستم مدیریت امنیت اطلاعات

محتوای استانداردهای BS7799، ISO/IEC 17799 و گزارش فنی ISO/IEC TR 13335، نشان می‌دهد که تمامی این استانداردها و گزارش‌های فنی، در کلیات مشترکند. تنها گزارش فنی ۱۳۳۳۵، با نگاهی فنی به پیاده‌سازی سیستم مدیریت امنیت اطلاعات پرداخته و جزئیات بیشتری رامطرح کرده است. لیکن با توجه به این‌که این گزارش فنی، اعتبار استاندارد را ندارد و فاقد تأییدیه‌های بین‌المللی است، لذا به‌منظور پیاده‌سازی موفق سیستم مدیریت امنیت اطلاعات در بانک‌ها و مؤسسات پولی و مالی، لازم است استاندارد BS7799 به‌عنوان مرجع اصلی مورد استفاده قرار گیرد و گزارش فنی ISO/IEC TR ۱۳۳۳۵ به‌عنوان

راهنمای فنی در مواردی که کلیات آن در استاندارد مذکور ارائه شده است، مورد استفاده قرار گیرد.

به علت اهمیت بالای مدیریت مخاطره[1] در برقراری امنیت اطلاعات و با توجه به شکل۲ این‌گونه دیده می‌شود که یک گام اصلی در چارچوب امنیت اطلاعات مؤسسه پولی و مالی، مدیریت مخاطره می‌باشد. در بخش بعدی به توضیحاتی راجع به این فرآیند می‌پردازیم.

۶- مفاهیم مدیریت خطرات امنیتی

در بسیاری از مؤسسات پولی و مالی، ضرورت توجه به "مدیریت خطرات امنیّتی" وقتی احساس می‌شود که یک مشکل مثل آلودگی یک رایانه به یک ویروس و یا حمله به یک وب سایت و نظایر آن بوجود آید. وقتی تعداد این حملات و آسیب‌ها زیاد می‌شوند، مؤسسات پولی و مالی ناامید شده و به‌جای برخوردهای منطقی، برخوردهای انفعالی را در دستور کار قرار می‌دهند.

افزایش بی‌رویه حملات به اصطلاح ویروسی، ضرورت پیاده‌سازی یک سیستم کارآمد و پیشگیرانه را برای مقابله با خطراتی از این دست اجتناب ناپذیر می‌کند.

مدیریت خطرات امنیتی، فرآیندی است که در آن تهدیدهای موجود در یک مؤسسه پولی و مالی شناسایی، اولویت‌بندی و نحوه مدیریت آنان در یک سطح قابل قبول مشخص می‌شود. وجود یک استراتژی مدون به‌منظور مدیریت خطرات امنیتی، مؤسسات پولی و مالی را قادر می‌سازد که فرآیندهایی را به‌منظور شناسایی و اولویت‌بندی فعالیت‌ها در محیط فن‌آوری اطلاعات پیاده‌سازی و از آنان نگهداری کنند.

جایگزینی برخوردهای پیشگیرانه با برخوردهای انفعالی، مهمترین دستاورد مدیریت خطرات امنیتی در یک مؤسسه پولی و مالی است که قطعاً بهبود وضعیت آن را به دنبال خواهد داشت چرا که احتمال دستیابی مستمر به زیرساخت فن‌آوری اطلاعات افزایش یافته و در فرآیندهای جاری یک مؤسسه پولی و مالی خللی ایجاد نمی‌کند.

پیاده‌سازی فرآیند مدیریت خطرات امنیتی برای مؤسسات پولی و مالی دستاوردهای متعددی را به دنبال خواهد داشت.

[1] Risk Management

- *زمان پاسخ به تهدیدات*

با ایجاد فرآیند مدیریت خطرات امنیتی، مؤسسات پولی و مالی می‌توانند در مقابل تهدیدات امنیتی جدید در زمان مناسب و به‌سرعت، و قبل از سوء استفاده از تمام محیط شبکه، واکنش لازم را نشان دهند. مدیریت خطرات امنیتی، بستر لازم برای پیشگیری در مقابل تهدیدها و یا آسیب‌پذیری مؤسسات پولی و مالی را فراهم می‌کند. بدین‌ترتیب، نحوه برخورد بانک‌ها و مؤسسات پولی و مالی با مسائل و مشکلات امنیتی از واکنش‌های انفعالی به واکنش‌های پیشگیرانه تغییر خواهد کرد.

- *مدیریت قانونمند*

تدوین مجموعه قوانین جدید در ارتباط با حفظ حریم خصوصی کاربران، تعهدات مالی و وظایف حقوقی، مؤسسات پولی و مالی را مجبور می‌کند که زیرساخت فن‌آوری اطلاعات خود را با دقت بیشتر و مؤثرتر از گذشته مدیریت کنند. بسیاری از مؤسسات پولی و مالی دارای تعهدات قانونی به‌منظور پیاده‌سازی و نگهداری یک سطح امنیتی حداقل در محدوده عملیاتی خود می‌باشند. بروز اشکال در مدیریت پیشگیرانه امنیتی، بانک‌ها و مؤسسات پولی و مالی را به‌دلیل عدم انجام وظایف و مسئولیت‌های قانونی خود در معرض آسیب حقوقی قرار خواهد داد.

- *هزینه‌های مدیریت زیرساخت*

فرآیند مدیریت خطرات امنیتی، مؤسسات پولی و مالی را قادر می‌سازد که با یک وضعیت مطلوب، مقرون به‌صرفه و در یک سطح قابل قبول امنیتی فعالیت‌های جاری خود را انجام دهند. فرآیند فوق همچنین یک مسیر مشخص و پایدار برای سازماندهی و اولویت‌بندی منابع محدود را به‌منظور مدیریت خطرات ارائه می‌کند. مزایای واقعی پیاده‌سازی مدیریت خطرات امنیتی زمانی آشکار می‌شود که مؤسسات پولی و مالی بتوانند کنترل‌هایی مقرون به‌صرفه به‌منظور کاهش تهدیدات امنیتی را پیاده‌سازی نمایند.

- مدیریت و اولویت‌بندی خطرات

مدیریت خطرات امنیتی می‌تواند به یک مؤسسه پولی و مالی کمک کند که اصول امنیتی را به‌منظور کاهش بیشترین خطرات در محیط مربوطه به‌کار گیرد (نه این‌که از یک رویکرد غیرمنسجم برای ایمن‌سازی عناصر مجزاء در مؤسسه پولی و مالی استفاده کند.

۷- رویکردهای متفاوت مدیریت خطرات امنیتی

اکثر سازمان‌ها به‌منظور مدیریت خطرات امنیتی از دو رویکرد متفاوت استفاده می‌کنند.

رویکرد انفعالی، فرآیندی است که براساس آن صرفاً پس از بروز یک حادثه امنیتی به آن پاسخ داده می‌شود. تعداد زیادی از کارشناسان حرفه‌ای فن‌آوری اطلاعات همواره با این محدودیت مواجهند که فعالیت‌ها را به‌گونه‌ای انجام و به‌اتمام برسانند که کمترین مشکل را برای کارکنان ایجاد نماید. پس از بروز یک مشکل امنیتی، کارشناسان فن‌آوری اطلاعات صرفاً می‌توانند از پیشرفت مشکل جلوگیری کرده و پس از ایزوله نمودن آن، مشکل سیستم‌های آلوده را برطرف کند. شاید در این رابطه برخی علاقه‌مند باشند که عامل اصلی بروز مشکل را پیدا نمایند، ولی با توجه به محدودیت زمان و منابع موجود در مؤسسه پولی و مالی، عملاً امکان انجام آن وجود نخواهد داشت. متأسفانه برای بسیاری از بانک‌ها و مؤسسات پولی و مالی همچنان رویکردهای انفعالی یک نگرش مؤثر به‌منظور برخورد با تهدیدات امنیتی است (پس از بروز مشکل در رابطه با نحوه برخورد با آن تصمیم گرفته می‌شود و برای پیشگیری از بروز حوادث از رویکرد خاصی تبعیت نمی‌شود).

رویکرد پیشگیرانه، فرآیندی است که باعث کاهش خطر آسیب‌پذیری در یک مؤسسه پولی و مالی می‌شود. مدیریت پیشگیری از خطرات امنیتی دارای مزایای متعددی نسبت به یک رویکرد انفعالی است. در مقابل این‌که منتظر بمانیم تا یک حادثه اتفاق افتد و به آن پاسخ دهیم، احتمال بروز مشکل در اولین مکان را کاهش خواهیم داد. بدین‌منظور از رویه‌هایی خاص به‌منظور حفاظت از سرمایه‌های مهم مؤسسه پولی و مالی استفاده می‌شود. با پیاده‌سازی کنترل‌هائی که کاهش آسیب‌پذیری سیستم و سوء استفاده از آنان توسط نرم‌افزارهای مخرب را به‌دنبال خواهد داشت، امکان سوء استفاده مهاجمان از فرصت‌های ایجاد شده کاهش یافته و پیشگیری لازم در این خصوص انجام خواهد شد.

یک رویکرد پیشگیرانه می‌تواند به یک مؤسسه پولی و مالی در جهت کاهش تعداد حوادث امنیتی در آینده کمک کند ولی این بدین‌معنی نخواهد بود که چنین مسائلی در آینده اتفاق نخواهند افتاد. بنابراین، مؤسسات پولی و مالی می‌بایست فرآیند پاسخ به حوادث امنیتی را بهبود داده و به‌طور همزمان ایجاد رویکردهای پیشگیرانه درازمدت را در دستورکار خود قرار دهند.

به این جهت که بانکداری الکترونیک درگاهی مجزا و نفوذپذیرتر از سایر کانال‌ها در صنعت بانکداری می‌باشد، به‌طوراخص به امنیت بانکداری الکترونیک می‌پردازیم.

۸- امنیت در بانکداری الکترونیک

روش‌های حفاظت امنیتی که توسط بانک‌ها پیشنهاد می‌شود و مشتریان نیز انتظار آن‌ها را دارند، شامل موارد ذیل است:

- واضح و مشخص بودن آدرس دقیق وب سایت تأیید شده مؤسسه پولی و مالی در نشریات بانک.
- تأیید و تصدیق وب سایت از طریق گواهینامه‌های دیجیتالی.
- نمایش شواهد حفاظت‌های امنیتی در صفحه نمایش (مثل آیکون قفل).
- حفاظت PIN و رمز عبور
- استفاده از صفحه کلیدهایی با محرک mouse یا لمسی برای اطلاعات حساس.
- محافظت در مقابل ویروس‌ها
- رمزگزاری حداقل ۱۲۸ بیتی
- پیاده‌سازی دیواره آتش
- قراردادن محدودیت برای مشتریانی که در وب سایت شناسائی نشده‌اند و محدودیت در دسترسی به کدها

موارد زیر برای افزایش اعتماد کاربران تجارت الکترونیک و بانک الکترونیک در جهت انجام فعالیت‌های اقتصادی و تجاری، مطرح می‌شود:

- محافظت- Protection:

فرآیندی که طی آن مشخص می‌شود کدام مشتریان متقاعد می شوند تا اطلاعاتشان بقدر کفایت توسط گردآورندگان اطلاعات جمع آوری شود.

- تأیید - Verification :

از آنجائی‌که به‌راحتی می‌توان نمونه‌های گوناگونی از یک وب سایت تهیه کرد، با استفاده از امکان اشتباه در نام دامنه وب سایت و یا موارد مشابه آن، امکان سوء استفاده بسیاری از افراد سودجو مهیا می‌شود؛ به‌طور مثال مشتری به‌جای پسوند com. از پسوند net. استفاده نماید و یا یکی از حروف را اشتباه تایپ کند مثلا حرف "y" را "i" درج کند.

منظور از تأیید، اطمینان دادن به مشتری از این جهت است که تراکنش‌هایی که از طریق وب سایت انجام می‌دهد با سایت واقعی و اصلی بانک مورد نظرش صورت گرفته باشد.

- تصدیق- Authentication:

منظور از تصدیق این است که یک گروه سوم (شخص ثالث) به‌عنوان ناظر حضور داشته باشد تا گواهی دهد که تراکنش‌ها بین چه افرادی صورت گرفته است و به‌عبارتی فعالیت در اینترنت از این طریق گارانتی شود.

- رد انکار- Non-Repudiation:

مکانیسمی برای اطمینان از این است که کامپیوتر Client (مشتری) با سرور بانک ارتباط برقرار نموده است و بالعکس. به این ترتیب گروه‌های شرکت کننده در این ارتباطات قادر به انکار فعالیت خود نخواهند بود.

۹- مراحل فرآیند تهیه یک قالب کاری[1]

قالب کاری که در ادامه راجع به آن بحث خواهیم کرد نیازمندی‌های امنیتی برای محیط بانکداری اینترنتی را پوشش می‌دهد، که البته این مدل توسعه‌یافته مدل تجارت الکترونیکی (E-Commerce) است.

۱- فهرست نمودن تمام نیازمندی‌های امنیتی برای محیط بانکداری اینترنتی به‌صورت‌کلی.
۲- مشخص نمودن تمام ذینفعان و شرکت‌کنندگان در فرآیند بانکداری اینترنتی.
۳- تجزیه تراکنش‌ها به چندین فعالیت کوچکتر و اتمیک.
۴- نگاشتن هر یک از این فعالیت‌ها به شرکت کنندگانی که آن را انجام خواهند داد، بدین ترتیب یک مدل برای بانکداری اینترنتی فراهم خواهد شد.
۵- استفاده از اطلاعات به‌دست آمده در مرحله ۴ جهت مشخص نمودن نیازمندی‌های بانکداری اینترنتی.
۶- از این نیازمندی‌های امنیتی برای توسعه معماری امنیتی، رویه‌های امنیتی مناسب و مکانیسم‌ها و سیاست‌ها استفاده می‌کنیم.

[1] Framework

جدول۲: طبقه‌بندی مفهومی برای اعتماد مشتریان به تراکنش‌ها در EC (تجارت الکترونیک)

	Protection **محافظت**	**Verification** **تأیید**	**Authentication** **تصدیق**	**Non-repudiation** **رد انکار**
آسیب پذیری	نفوذ به مقصد و یا منابع	تغییر شکل وب سایت	جازدن خود به‌عنوان فرد اصلی	برقراری ارتباط با گروهی که بعداً به دروغ تراکنش انجام شده رد شود.
روش مقابله	افشاء خط مشی‌ها با توجه به روش محافظت و جمع آوری اطلاعات	پورتال، مانندwww.yaho.com برای تعیین نام دقیق دامنه وب سایت	وجود شخص ثالث بی‌طرف مثل Verisign www.verisign.com برای صحه گذاشتن به افرادی که وارد وب سایت می‌شوند.	مکانیسم‌هائی برای اطمینان کلاینت (مشتری) از اتصال به سرور بانک (سرور اصلی) و یا بالعکس
فناوری پیاده‌سازی	تکنولوژی‌هایFireWall	_____	مبادله نمودن گواهینامه دیجیتالی با رمزگزاری	امضاهای دیجیتالی

در جدول ۲ آسیب‌پذیری، روش مقابله و فناوری پیاده‌سازی موارد ذکر شده دیده می‌شوند.

۱۰- نیازمندی‌های امنیتی محیط بانکداری اینترنتی در حالت کلی

۸ مورد امنیتی زیر برای E-Commerce تعریف می‌شود:

۱- تعیین و تأیید هویت– Identification and authentication : شناسایی هرکاربر به‌صورت منحصر به‌فرد و اثبات آن.

۲- اجازه دادن– Authorisation : توانایی کنترل فعالیت‌هایی که هر کاربر براساس هویتی که برایش تعریف شده است، انجام می‌دهد.

۳- اعتماد – Confidentiality : ممانعت از دخالت افراد یا اطلاعات‌گیری آنهایی که اجازه دسترسی ندارند.

۴- یکپارچگی- ntegrity : قدرت اطمینان دادن از این‌که اطلاعات به‌صورت تصادفی و یا توسط افرادی که حق دسترسی ندارند، تغییر داده نخواهد شد.

۵- رد انکار - Non-Repudiation: ممانعت از انکار توسط کاربران.

۶- دسترس پذیری - Availability: تهیه خدمات بدون وقفه.
۷- خط مشی- Privacy: ممانعت از استفاده غیرقانونی و یا غیرحقوقی اطلاعات و داده‌ها.
۸- بازبینی کردن- Auditability: نگهداری رکورد تمامی تراکنش‌های رخداده برای اصلاح و یا بازبینی.

برای توسعه این موارد برای محیط بانکداری اینترنتی نیاز داریم تا مکانیسم‌های تصدیق و تأیید را از روش Corner-stone (به‌طور اساسی) انجام دهیم به این معنا که از رمزهای عبور، کارت‌ها و قابلیت‌های بیومتری برای شناخت استفاده کنیم.

۱۱- محیط بانکداری اینترنتی

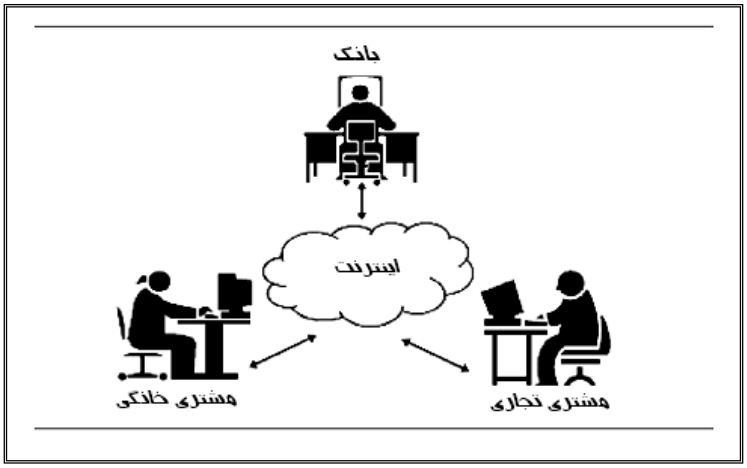
۳ محیط اصلی در فضای بانکداری اینترنتی وجود دارند: بانک، اینترنت، کاربر کامپیوتر(مشتری با فعالیت تجاری خانگی و یا بانکی)

شکل زیر نمای ساده‌ای از فرآیند تراکنش در بانکداری اینترنتی را نمایش می‌دهد که در آن مشتری مایل به پرداخت صورتحساب می‌باشد.

۱-۱۱- حوزه اول: مشتری خانگی

امکان دارد این نوع مشتری در هر مکانی باشد و یا از هر نوع مکانیسم امنیتی استفاده کند، ولی تنها تخمینی که راجع به او می‌توان زد این است که اغلب مشتریان خانگی از جستجوگرهایی در اینترنت استفاده می‌کنند که پشتیبان گواهینامه‌های دیجیتالی و SSL هستند. چون بیشترین جمعیت استفاده کننده از بانکداری اینترنتی کاربران خانگی هستند پس محیط بانکداری اینترنتی باید user-friendly و امن باشد و قدرت هرگونه تراکنش را برای آنان داشته باشد.

شکل ۳: محیط بانکداری اینترنتی



از شکل۳، ۴ حوزه معین می‌شود.

۲-۱۱- حوزه دوم: مشتری تجاری

بزرگترین تفاوتی که بین مشتریان خانگی و مشتریان تجاری وجود دارد پیاده‌سازی برخی اشکال مکانیسم‌های امنیتی است.

در این حوزه دو نقش ایفا می‌شود: یکی نقش مشتری، یعنی مشتری تجاری هم مانند مشتری خانگی با بانک ارتباط دارد و نقش دوم به‌عنوان تاجر که بین بانک و مشتری قرار می‌گیرد، که در این صورت باید مسئولیت تراکنش‌هایی را که مشتری تا قبل از پاس شدن به بانک انجام می‌دهد به‌عهده گیرد.

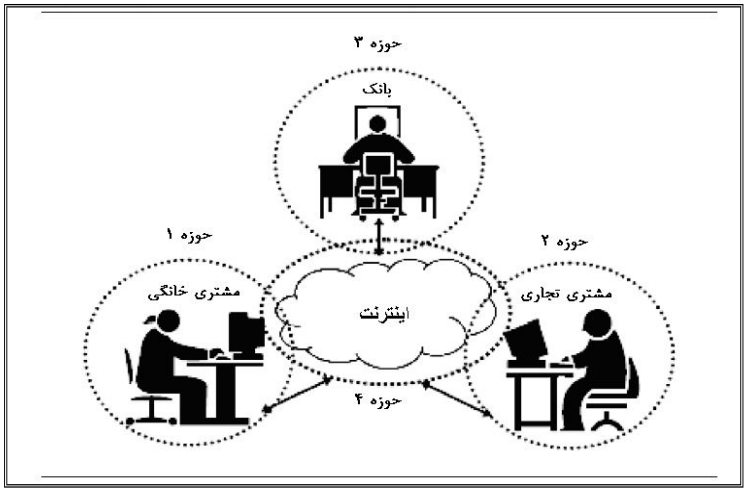
۳-۱۱- حوزه سوم: بانک

بانک در این حوزه ۲ نقش دارد: شناسایی مشتری و تعیین حق دسترسی وی به اطلاعات برای اطمینان خاطر و ایمن‌بودن در جهت رفع انکار.

۴-۱۱- حوزه چهارم: اینترنت

چهار حوزه بحث شده در شکل ۴ دیده می‌شوند.

شکل۴: حوزه‌ها در محیط بانکداری اینترنتی



۱۲- فعالیت‌های اتمیک تراکنش‌های بانکداری اینترنتی

در شکل ۵ فعالیت‌های اتمیک تراکنش‌های بانکداری اینترنتی با ذکر شماره دیده می‌شوند.

۱- مشتری، از فضای اینترنت برای ارتباط با وب سایت بانک مربوطه استفاده می‌کند.

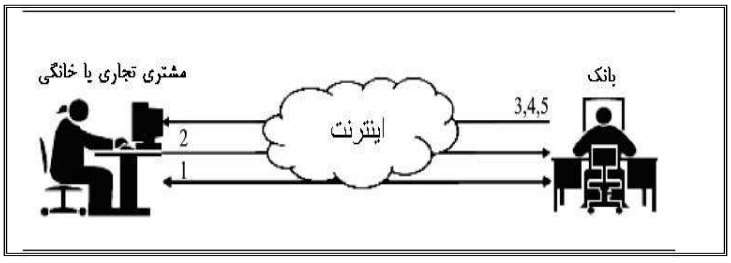
۲- مشتری، وب سایت را جستجو و خدمات مورد نظرش را انتخاب می‌کند. تراکنش اینترنتی با تهیه صورتحساب و اطلاعات پولی مشتری شروع می‌شود.

۳- بانک، کنترل می‌کند که آیا عملیات درخواست شده توسط مشتری با توجه به وضعیت مالی وی قابل انجام است یا خیر و پاسخ آن را به مشتری برمی‌گرداند.

۴- در همان آن تأیید تراکنش برای مشتری ارسال می‌شود.

۵- بانک، عملیات مالی را برای مشتری انجام می‌دهد و رسید انجام آن را بر می‌گرداند.

شکل۵: فعالیت‌های اتمیک تراکنش‌های بانکداری اینترنتی



۱۳- تحلیل تصمیم‌گیری‌های امنیتی

در جدول۳ ، فعالیت ۱ نشان می‌دهد که بانک باید قادر به شناسایی هویت مشتری و تأیید وی جهت انجام عمیات باشد و مشتری خواهان Privacy (محرمانه بودن) اطلاعات فردیش می‌باشد. فعالیت‌های۴ و ۵ احتیاج به این دارند که بانک تأیید انجام عملیات را ارسال و امنیت اعتماد و یکپارچگی را تضمین کند و همزمان با آن مشتری گارانتی‌ای را خواستار است تا بعداً بانک نتواند عملیات انجام شده را رد کند. که این همان امنیت رد انکار می‌باشد. در جدول۳، نشان داده شده که بانک باید تراکنش‌ها را جهت بازبینی مجدد و اصلاح، ثبت کند.

جدول۳: جدول تصمیم‌گیری (۱۳)

		مرحله3 فعالیت ها									
	حوزه ها	1	2	3	4	5					
مرحله 2	مشتری	X	X		X						مرحله 4 تراکنش
	اینترنت	X	X								
	بانک	X		X		X					
	نیازمندیهای امنیتی										
مرحله 1	تعیین و تائید هویت	X	X								مرحله 3 قلب کاری برای امنیت
	اجازه دادن			X							
	اعتماد		X		X	X					
	یکپارچگی		X		X	X					
	رد انکار		X		X	X					
	دسترس پذیری				X						
	محرمانه بودن	X									
	بازبینی کردن			X		X					

۱۴- امنیت اطلاعات در سازمان‌ها طی سالیان اخیر

ماحصل بررسی انجام شده توسط مؤسسات و مراکز تحقیقاتی معتبر درخصوص امنیت اطلاعات، نشان‌دهنده این واقعیت مهم است که حملات مهاجمان بر روی درآمد و هزینه یک مؤسسه پولی و مالی به‌طور مستقیم و یا غیرمستقیم تأثیر خواهد داشت (کاهش درآمد، افزایش هزینه).

با این‌که هزینه پیاده‌سازی یک سیستم حفاظتی کم نیست اما می‌توان آن را به‌عنوان بخشی از هزینه‌هایی در نظر گرفت که یک مؤسسه پولی و مالی به‌دلیل عدم ایمن‌سازی، باید پرداخت کند (برخورد با تبعات منفی). مؤثرترین راهکار و یا راه حل امنیتی، ایجاد یک محیط چندلایه‌ای است. در یک محیط چندلایه، مهاجمان در هر لایه شناسایی و با آنان برخورد خواهد شد. موفقیت یک مهاجم نیز به عبور موفقیت‌آمیز از هر لایه بستگی دارد.

راهکار امنیتی چندلایه به "دفاع در عمق" نیز مشهور است. در این مدل، در هر لایه، از استراتژی‌های تدافعی خاصی استفاده می‌گردد که با توجه به ماهیت پویای امنیت اطلاعات، می‌بایست به‌صورت ادواری توسط کارشناسان حرفه‌ای امنیت اطلاعات، بررسی و به‌هنگام گردند.

در سال ۲۰۰۴، هفتاد درصد سازمان‌ها حداقل یک مرتبه مورد تهاجم قرار گرفته‌اند.

در سال ۲۰۰۳ بالغ بر۶۶۶ میلیون دلار صرف برخورد با مشکلات امنیتی در سازمان‌ها شده است.

بر اساس آمار منتشر شده در سایت گروه کاربران بین‌المللی سیستم مدیریت امنیت اطلاعات (ISMS IUG)[1] تا آوریل سال ۲۰۰۷ مجموعا تعداد ۳۵۴۰ سازمان در سطح جهان، موفق به اجرای ISMS براساس این استاندارد و اخذ تأییدیه از مراکز صدورگواهی مبتنی بر این استاندارد شده‌اند. از این تعداد ۱۲۳۵ مورد مربوط به ISO/IEC 27001 می‌شود که از بین آن‌ها ۶۵۶ مورد مربوط به استاندارد BS7799 قسمت دوم سال ۲۰۰۲ و ۵۹۷ مورد تأییدیه‌های جدید می‌باشد.

نیمی از سازمان‌ها به این موضوع اعتراف کرده‌اند که نمی‌دانند چه میزان از اطلاعات سازمان خود را به دلیل حملات از دست داده‌اند.

چهل و یک درصد سازمان‌ها اعلام کرده‌اند که دارای هیچگونه طرح و یا برنامه‌ای برای گزارش و یا پاسخ به تهدیدات امنیتی نیستند.

[1] Information Security Management System

نتیجه‌گیری

بانک‌ها، مؤسسات پولی و مالی و مؤسسات تجاری با پیاده‌سازی یک استراتژی امنیتی از مزایای زیر بهره‌مند خواهند شد:

- افزایش مشتریان بانکی و بانکداری الکترونیک با افزایش اطمینان مشتریان به مؤسسه پولی و مالی.
- سودآوری بیشتر مؤسسات پولی و مالی با جذب سرمایه‌های مشتریان افزوده شده.
- کاهش احتمال غیرفعال شدن سیستم‌ها و برنامه‌ها (از دست‌دادن فرصت‌ها).
- استفاده مؤثر از منابع انسانی و غیرانسانی در یک مؤسسه پولی و مالی (افزایش بهره‌وری) کاهش هزینه از دست دادن داده توسط ویروس‌های مخرب و یا حفره‌های امنیتی (حفاظت از داده‌های ارزشمند).
- افزایش حفاظت از مالکیت معنوی.
- دارا بودن یک استراتژی برای مدیریت مخاطرات در مواقع لازم.

یک مشکل امنیتی که باعث از بین رفتن اطلاعات مشتریان می‌شود، می‌تواند پیامدهای قانونی برای یک مؤسسه پولی و مالی به‌دنبال داشته باشد.

منابع و مآخذ

دشتی، افسانه. خـرداد ۱۳۸۴."***شبکه اطلاع رسانی ماهنامــه شــبکه. اســتانداردهای امنیت ـ آشنایی با استاندارد BS۷۷۹۹***". ماهنامه شبکه. شماره۵۴.

http://www.shabakeh-mag.com/Articles/Show.aspx?n=1001277

http://www.iso27001certificates.com

British Standard Institute. 1999."***Information security management- part 1: code of practice for information security management (BS 7799-1)***".

British Standard Institute. 1999. "***Information security management- part 2: specification for information security management (BS 7799-2)***".

International Standard Organization. 2000. "***Information technology- Code of practice for information security management (ISO/IEC 17799)***".

ISO/IEC 17799:2000."***Code of Practice for Information Security Management, Frequently Asked Questions***".What is ISO/IEC 17799:2000,November2002,availableat.
http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf

International Standard Organization. 1996. "***Information technology- Guidelines for the management of IT security- Part 1: Concepts and models for IT security (ISO/IEC 13335-1)***".

International Standard Organization. 1997. "***Information technology- Guidelines for the management of IT security- Part 2: Managing and planning IT security (ISO/IEC 13335-2)***".

International Standard Organization.1998."***Information technology- Guidelines for the management of IT security- Part 3: Techniques for the management of IT security (ISO/IEC 13335-3)***".

International Standard Organization.2000."***Information technology- Guidelines for the management of IT security- Part 4: Selection of safeguards (ISO/IEC 13335-4)***".

International Standard Organization. 2001."***Information technology- Guidelines for the management of IT security- Part 5: Management guidance on network security (ISO/IEC 13335-3)***".

Eeye Digital Security and ECSC Ltd Whitepaper, Attaining BS7799 Compliance with Retina Vulnerability Assessment Technology, "***Information Security Risk Assessments The Special Case of IT Vulnerability Assessments***". Available at www.ecsc.co.uk/pdf/ECSC-eEye-Whitepaper.pdf

Hutchinson, D. and Warren, M. "***Security for Internet banking: a framework***" Journal of Enterprise Information Management, Vol 16, No 1, pp. 64-73, Emerald, United Kingdom. 2003.