بررسی و آگاهی‌بخشی استانداردها در حوزهٔ امنیت اطلاعات

مینا فیلی و منصور اسماعیل‌پور*

دانشجوی دکترای مدیریت فناوری اطلاعات، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران
feili_mina@yahoo.com
گروه مهندسی کامپیوتر، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران
esmaeilpour@iauh.ac.ir

چکیده

تدوین استاندارد در حوزهٔ امنیت فناوری اطلاعات، به‌تبع جوان‌بودن این حوزه، موضوعی به‌نسبت جدید است؛ اما می‌توان گفت که سابقهٔ طولانی فرآیند استاندارد، منجر به تدوین استانداردهایی پخته و کارآمد در این حوزه شده است. چشم‌پوشی از امنیت اطلاعات به منزلهٔ بازکردن آغوش بر روی انواع مشکلات و مسائل پرمخاطره است که ممکن است در انجام هر کاری با آن روبه‌رو شد. امنیت اطلاعات نقش مهمی در محافظت از دارایی‌های سازمان دارد. با توجه به این‌که هیچ فرمولی نمی‌تواند امنیت را به‌طور کامل تضمین کند، به‌هرحال به یک‌سری معیارها و استانداردها برای دست‌یابی به سطح مناسبی از امنیت اطلاعات نیاز داریم تا منابع سازمان به‌طور مؤثر مورد استفاده قرار گرفته و بهترین شیوهٔ امنیتی اتخاذ شود. مطالعهٔ کارهایی که در زمینهٔ امنیت اطلاعات انجام شده، نشان داده که وسعت و پیچیدگی امنیت اطلاعات به‌حدی است که استانداردهای بسیاری در حوزهٔ امنیت اطلاعات ارائه شده‌اند و هر یک از آن‌ها یک جنبهٔ خاص از امنیت را پوشش داده است؛ حتی گاهی مجموعه‌ای از این استانداردها برای پوشش‌دادن تنها یک جنبه از امنیت اطلاعات ارائه شده است. در به‌کارگیری استانداردهای امنیت اطلاعات، ابتدا باید به مطابقت با استاندارد اصلی تأکید کنیم و توجه داشته باشیم که بومی‌سازی یا متناسب‌سازی آنها ممکن است معضلاتی به‌وجود بیاورد. در این نوشتار برآنیم به معرفی استانداردهای امنیت اطلاعات در دنیا بپردازیم و نحوهٔ تغییر دیدگاه‌های بررسی امنیت اطلاعات به‌تفصیل مورد بررسی قرار خواهد گرفت که در این مسیر به معرفی ابزارها و راه‌کارهای مختلفی پرداخته می‌شود.

واژگان کلیدی: امنیت اطلاعات، آگاهی اطلاعاتی، استانداردها امنیت اطلاعات، تهدید، مخاطرات امنیتی

۱- مقدّمه

پدیدهٔ امنیت اطلاعات یکی از دلایلی است که تأمین امنیت اطلاعات را به یک مقولهٔ مهم تبدیل کرده است. بدون سعی و تلاش برای تداوم امنیت اطلاعات و نگه‌داشتن سازمان در سطح قابل قبولی از حفاظت اطلاعات، تمام هزینه‌های صرف‌شده برای امنیت اطلاعات ارزش خود را از دست داده و عدم امنیت نسبت به اطلاعات رخ خواهد داد.

در سازمان‌ها هزاران قواعد و مقررات برای تأمین امنیت اطلاعات به کار گرفته می‌شود. این مقوله گاهی با اصطلاحاتی نظیر "امنیت" و "حفاظت" شناخته می‌شود؛ اما در موارد بسیاری با استفاده از عباراتی که با مشخصه‌های امنیتی مرتبط هستند، مثل قابلیت اعتبار، یکپارچگی، صحت و دردسترس‌بودن اطلاعات بیان می‌شوند.

امنیت به‌خودی‌خود هدف نیست، بلکه یک ویژگی خاص هر سازمان است. در مورد امنیت اطلاعات، آنچه برای یک سازمان مناسب است، به‌حتم نباید برای سازمان دیگر به‌کار گرفته شود و حتی می‌تواند برای سازمانی دیگر مخاطره‌آمیز باشد. بنابراین هر سازمانی نیاز ضروری و قطعی به امنیت طراحی‌شدهٔ خاص خود دارد؛ لذا تقویت و ثبات در اجرای استانداردها از جمله موارد مربوط به نگهداشت امنیت اطلاعات در هر سازمانی است [۱].

۱-۱- امنیت اطلاعات[1]

در فرهنگ لغت امنیت سامانه‌های اطلاعات ملی امریکا در تعریف امنیت چنین آمده است:

[1] Information Security

* نویسندهٔ عهده‌دار مکاتبات

"محافظت از سامانه‌های اطلاعاتی در مقابل دسترسی غیر مجاز یا اصلاح اطلاعات در هریک از مراحل مختلف ذخیره‌سازی، انتقال و یا پردازش و همچنین محافظت در مقابل عدم ارائهٔ خدمات به کاربران مجاز و یا ارائهٔ خدمات به کاربران غیر مجاز، و همچنین اقداماتی که لازم است برای تشخیص، مستندسازی و مقابله با تهدیدات انجام داد" [۳].

برخی از سازمان‌های دولتی و غیر دولتی استانداردها و معیارها و در برخی موارد قوانین و مقرراتی را برای امنیت اطلاعات وضع کرده‌اند تا اطمینان حاصل کنند سطح مناسبی از امنیت را در داخل سازمان برقرار کرده و منابع اطلاعاتی نیز در مسیر درست استفاده می‌شود. در این خصوص سعی می‌شود، بهترین شیوهٔ امنیتی اتخاذ شود. برخی شرکت‌ها مثل بانک‌ها، مقررات، راه‌کارها و شیوه‌هایی را باهم استفاده می‌کنند به‌طوری‌که به‌عنوان بخشی از مقررات سازمانی در سازمان اعمال می‌شود.

برخی معتقدند امنیت اطلاعات ۲۰٪ جنبهٔ فنی و ۸۰٪ جنبه رفتاری دارد و برخی نیز نسبت آن را ۱۰ به ۹۰ می دانند. نتیجه یک پژوهش در سال ۲۰۰۳[1] نشان داد که ۳۰٪ امنیت فناوری اطلاعات به فناوری بر می‌گردد و ۷۰٪ به رفتار کارکنان بستگی دارد [۲].

دول توسعه‌یافته در جهان به‌تدریج وابستگی ساختار اجتماعی و اقتصادی خود به شبکه‌های اطلاعاتی، به‌خصوص اینترنت را تشخیص می‌دهند. آنها بنیان آماری خود را به‌عنوان دارایی ملی و استراتژیک خود در نظر می‌گیرند. دو نمونه مصداق این گفته عبارتند از:

- آژانس بین‌المللی امنیت شبکه و اطلاعات اروپا بر اهمیت امنیت اطلاعات در اقتصا اروپا تأکید کرده و اقدامات متمرکز در جهت اجتناب از رقم ۱۱/۹ را لازم دانست.

به‌منظور تکمیل این مطلب، به چند نمونه از ابتکارات در توسعهٔ امنیت اطلاعات به‌عنوان یک رشتهٔ تخصصی اشاره می‌کنیم. بسیاری از دول در حال تصویب لوایحی به‌منظور توانمندسازی توابع امنیت اطلاعات و ایجاد قابلیت‌های امنیت اطلاعاتی ارتجاعی در خدمات دولتی و نیروهای نظامی خود هستند که بیشتر به شکل مؤسسات امنیت اطلاعات ملی و گروه‌های واکنش اضطراری هماهنگ (CERTs) اجرا می‌شوند [۵].

[1] AT&T Network Security survey from March/April Meta Group ,2003

دو نمونه از این ابتکارات عبارتند از:

قانون اصلاح پژوهش و توسعهٔ امنیت شبکه‌ای سال ۲۰۰۹ در آمریکا با تصویب اعتباری به مبلغ هفت میلیون دلار آمریکا در سال ۲۰۱۰ و افزایش این رقم به نود میلیون دلار آمریکا تا سال ۲۰۱۴ برای پژوهش در زمینهٔ امنیت شبکه و سامانه‌های رایانه‌ای. اتحادیهٔ اروپا بودجه‌ای به مبلغ ۷.۹۳ میلیون یورو به آژانس امنیت شبکه و اطلاعات اروپا (ENISA) برای سال ۲۰۰۹ اختصاص داد. در ادامه و در بخش دوم به معرفی استانداردهای مختلف دنیا و همچنین به بررسی ابزارها و تکنیک‌های مورد استفاده در بخش سوم، بررسی استانداردها در محافل علمی در بخش چهارم و زیرساخت‌ها در بخش پنجم و سپس در بخش ششم به بررسی مواردی در ایران پرداخته می شود.

۱-۲- استانداردها و رویه‌های بین‌المللی امنیت اطلاعات

معماری نیازمندیهای امنیت اطلاعات سازمانی که به‌اختصار EISA[2] خوانده می‌شود، نخستین‌بار توسط گارتنر به‌عنوان یک برنامهٔ اثربخش امنیت اطلاعات در سازمان پیشنهاد شد. هدف از این معماری فراهم‌ساختن چهارچوبی بود که سازمان بتواند بر اساس آن، نیازمندی‌های امنیت اطلاعات تخصصی خود را شناسایی کرده، به تحلیل و ارزیابی آنها بر اساس اولویت‌بندی ریسک‌ها بپردازد تا بتواند نیازمندی‌های امنیت اطلاعات سازمان را مرتفع و در مورد بهترین راه‌حل‌های پیاده‌سازی یکپارچهٔ امنیت در سازمان و برای مدیریت ریسک‌های اطلاعاتی خاص سازمان تصمیم‌گیری کند.

۲- مروری بر بیست سال امنیت اطلاعات در دنیا

در طول بیست سال اخیر هر چیزی که فکرش را بکنید تغییر کرده، تغییراتی نه تنها ظاهری که حتی در بنیاد و باطن یک پدیده. برای مثال پدیدهٔ پیام‌رسانی فوری، کماکان به‌عنوان یک مفهوم و پدیدهٔ نوپا بود که ناگهان وب۲ متولد شد. پدیدهٔ پردازش‌های ابری در حال حاضر آن‌قدر نوپا و نوظهور هستند که هنوز بسیاری از مردم درک کامل و صحیحی از آن ندارند که درواقع چه هست، چه می‌کند و چه مزایا و معایبی دارد. شاید بتوان نخستین رویداد جدی

[2] EISA : Enterprise Information Security Assessment

شکل‌گرفته در حوزهٔ امنیت فناوری اطلاعات را به سال ۱۹۷۸ ارجاع داد. در این سال کنفرانس امنیت رایانه با موضوع بسط سیاست‌ها، برنامه‌ریزی‌های زمان بحران، امنیت فیزیکی مراکز داده و فناوری‌های جدید درخصوص سامانه‌های کنترل دسترسی مورد بحث وبررسی قرارگرفتند [۴].

حرکت به سمت تمرکززدایی، محققان وفعالان حوزهٔ امنیت رایانه را به سمت تغییر نگاه‌ها و سیاست‌هایی که تا پیش از این، در این حوزه اعمال می‌کردند، واداشت. درواقع باید سیاست‌ها را به‌گونه‌ای تغییر می‌دادند که نرم‌افزارها و سخت‌افزارهای امنیتی خود را با شرایط جدید که همانا گسترش سامانه‌های رایانه‌ای در بخش‌های مختلف بود، هم‌سو کنند؛ و شاید بتوان گفت از همین دوران بود که حتی شغل جدیدی با عنوان "کارمند امنیت سامانه‌های اطلاعاتی" [۱] ایجاد شد. در سال ۱۹۹۱، با معرفی گواهی‌نامه امنیت سامانه‌های اطلاعاتی[۲]، گام بسیار مهم و جدّی در توسعه و پیشرفت صنعت امنیت اطلاعات برداشته شد و امروزه با گذشت بیست سال از معرفی این گواهی‌نامه، دارنده آن به‌عنوان فردی که دارای سطح دانش و اطلاعات قابل قبول در حوزهٔ امنیت اطلاعات است، شناخته می‌شود و درواقع، داشتن سطح اطلاعات قابل قبول، یکی از عوامل کلیدی موفقیت در برنامه‌های امنیت اطلاعات است. بحث امنیت اطلاعات به‌قدری با اهمیت شده است که در بخش مدیریت ریسک سازمان‌ها و نهادها به آن پرداخته می‌شود[۳].

در گذشته بحث امنیت اطلاعات به‌طور عمده‌ای محدود به مسائل فنی و ابزارهایی بود که به حل مشکلات و مسائل حوزهٔ فناوری اطلاعات کمک می‌کردند و به‌طور اصولی این مباحث در پشت درهای بسته مطرح و حل می‌شدند و به‌ندرت به‌صورت علنی مطرح می‌شدند؛ اما بعدها با انجام تعدادی از حملات سایبری و البته ترکیب آنها با بعضی از بلایای طبیعی، بحث اعمال حاکمیت در موضوع امنیت اطلاعات در کانون توجهات قرار گرفت. دولت‌ها فعالیت‌های مثبتی نیز در راستای توسعهٔ بحث امنیت اطلاعات انجام داده‌اند، که ارائهٔ طرح‌ها و لوایح جدید برای بالابردن آگاهی عمومی و همچنین تدوین استانداردهای جدید دولتی در این خصوص قابل اشاره هستند. برخی از مشهورترین این قوانین، حمایت از سرمایه‌گذاران برای بهبود دقت و قابلیت اطمینان اطلاعات شرکت‌های بزرگ در ایالات متحده[۴] و قانون اطلاعات شخصی اروپا[۵] در کشورهای عضو اتحادیهٔ اروپا هستند. این نوع بازنگری درخصوص قوانین و اعمال حاکمیت‌های دولتی، خودبه‌خود منجر به ایجاد پست‌های سازمانی جدیدی چون مدیر ارشد امنیت اطلاعات[۶]، مدیر ارشد ریسک[۷] و مدیر ارشد حریم شخصی[۸]شد [۸].

۲-۱- توسعهٔ سیاست‌های امنیت اطلاعات

اگر به سال‌های ۱۹۸۰ تا ۱۹۹۰ نگاهی بیندازیم، خواهیم دید که در آن دوران همچنان در بحث توسعه و بسط سیاست‌های امنیت اطلاعات تلاش و کار چندان مهمی در شرکت‌ها و سازمان‌ها صورت نپذیرفته بود و درواقع تنها فردی که متولی و مسئول تدوین این سیاست‌ها بود. مدیر فناوری اطلاعات آن سازمان بود که وی نیز کار چندانی در این خصوص انجام نمی‌داد؛ اما درنهایت تصویب قوانین مختلف را می‌توان به‌عنوان سرآغاز ایجاد یک فرآیند ساخت‌یافته در جهت پیشبرد و تدوین سیاست‌هایی انسجام‌یافته درخصوص توسعهٔ امنیت اطلاعات در نظر گرفت؛ و البته در سال ۲۰۰۲ نیز ارائهٔ قانون حمایت ازسرمایه‌گذاران برای بهبودبخشیدن به دقت و قابلیت اطمینان شرکت‌های بزرگ[۹]توانست کمک شایانی به این امر کند [۶].

۲-۲- آزمایش نفوذ

انجام آزمایش‌های نفوذ، همچنان به‌عنوان یکی از مهم‌ترین آزمایش‌ها برای بررسی میزان آسیب‌پذیری سامانه‌های مرتبط با فناوری اطلاعات مطرح است. در طول دو دههٔ هفتاد و هشتاد به‌طور معمول بحث‌های مربوط به آزمایش‌های نفوذ، به‌عنوان یک سری از آزمایش‌های محرمانه در مراکز پژوهشی نظامی و دانشگاهی مد نظر بوده است. در اوایل دههٔ نود، زمانی که نخستین بذرها در جهت توسعهٔ اینترنت پاشیده شد و انقلاب فناوری اطلاعات در حال طلوع‌کردن بود، بحث انجام آزمایش‌های نفوذ نیز، به‌ناگاه دارای اهمیت فراوانی شد و نرم‌افزارها و استانداردهای فراوانی در این خصوص منتشر شدند [۱].

[1] ISSO: Information System Security Officer
[2] CISSP: Certified Information System Security Professional
[۳] در سی و ششمین کنفرانس سالانه موسسه امنیت اطلاعات نیز بحث مدیریت ریسک پر مباحثه ترین موضوعات بوده است

[4] SOX: Sarbanes – Oxely Act
[5] EU Data Privacy Act
[6] CISO: Chief Information Security Officer
[7] CRO: Chief Risk Officer
[8] CPO: Chief Privacy Officer
[9] SOX: Sarbanes–Oxely Act

۲-۳- محاسبات ابری و چالش‌های امنیتی

واژهٔ جدیدی به نام امنیت ابری به جمع واژگان مدیریت امنیت افزوده شده است که روش جدیدی و البته چالشی جدید برای کاربران ایجاد و امروزه محاسبات ابری توجهات زیادی را به خود جلب کرده است. محاسبات ابری این پتانسیل را دارد که در چند سال آتی روش انجام محاسبات در سازمان‌ها را تغییر دهد. مزایای محاسبات ابری به‌سادگی قابل شناسایی است؛ این روش، حافظهٔ بیشتر، انعطاف‌پذیری بیشتر و از همه مهم‌تر کاهش هزینه‌ها را به‌دنبال خواهد داشت. امتیازات بارز محاسبات ابری توجه بسیاری از سازمان‌ها را به خود جلب کرده است؛ اما جنبه‌ای که هنوز باعث عقب‌نشینی بسیاری از سازمان‌ها در برابر این فناوری می‌شود، نحوهٔ امن‌سازی داده‌ها در ابر و اطمینان از امنیت محیط است. فناوری ابری قادر است، داده‌های بسیاری از سازمان‌ها را در یک محیط اشتراکی ذخیره کند و درنتیجه هزینه‌ها را کاهش دهد [۷]. بنابراین داده‌های مشتریان در یک ابر در کنار هم قرار دارند. ارائه‌دهندهٔ سرویس ابر باید اطمینان حاصل کند که این داده‌ها جداسازی شده‌اند و ریسک‌های امنیتی کاهش یافته است. یک راه برای انجام این کار استفاده از روش‌های رمزنگاری برای رمزکردن داده‌ها و اعطای مجوز دسترسی به افراد خاص است.داده‌های حساس که در خارج از سازمان نگهداری می‌شوند، دارای یک ویژگی خطرناک امنیتی هستند. هرچه دید عمیق‌تری از ریسک‌های بالقوه داشته باشید، جلوگیری، کمینه‌کردن و کنترل این ریسک‌ها راحت‌تر خواهد بود. اتحادیهٔ اروپا استانداردهای جدیدی را برای انجام اقداماتی در جهت حمایت از گسترش محاسبات ابری تهیه کرده است. افزایش میزان بهره‌وری و صرفه‌جویی در تولید انبوه از طریق محاسبات ابری می‌تواند ۲.۵ میلیون شغل ایجاد کرده و ۱۶۰ میلیارد یورو به عبارتی حدود یک درصد به تولید ناخالص داخلی این اتحادیه تا سال ۲۰۲۰ بیافزاید. اجزای این استراتژی شامل تعیین استانداردهای فنی برای ایجاد قابلیت همکاری، قابلیت انتقال دیتا و برگشت‌پذیری تا سال ۲۰۱۳، راه‌اندازی طرح صدور گواهینامه در سطح اتحادیهٔ اروپا برای ارائه‌دهندگان سرویس ابری با امنیت بالا است. از دیگر بخش‌های این استراتژی توسعهٔ مدل " سالم و امن[1] "در عقد قرارداد با سرویس‌های ابری نظیر توافق نامه سطح خدمات و استفاده از توان خرید دولت‌ها و نهادهای بخش عمومی برای خرید خدمات ابری است. به گفتهٔ اتحادیه اروپا، طرح پیشنهادی برای به‌روزرسانی قوانین حفاظت از داده و برنامهٔ امنیت سایبری، همگی بخشی از تلاش‌های این اتحادیه برای یکپارچه سازی بازار سرویس‌های دیجیتال اتحادیه اروپا است [۹].

۳- انجمن‌های فعال در زمینهٔ امنیت اطلاعات در صنایع مختلف

ماهیت کنونی اطلاعات و سامانه‌های مبتنی بر فناوری اطلاعات، با حفظ اطلاعات ارزشمند آن، امنیت اطلاعات را به رکن اصلی در حفظ اطلاعات در بسیاری از بخش‌ها تبدیل می‌کند. برای متخصصان امنیت اطلاعات این یک مزیت بزرگی است که هرروز مورد توجه و تقاضای فعالان صنایع مختلف هستند.

۳-۱- شبکه‌سازی نظارتی امنیت اطلاعات

ایجاد شبکه‌های تخصصی متشکل از متخصصان امنیت اطلاعات از صنایع مختلف و کلیهٔ اعضای انجمن امنیت اطلاعات با تمایلات و اهداف متفاوت که به‌طور مشابه نسبت به دو ویژگی اصلی امنیت اطلاعات که امنیت اطلاعات نظارتی یا سیاستی و فنی مهارتی‌است، به‌طور هدفمند فعالیت می‌کنند.

۳-۲- کنسرسیوم تأیید امنیتی سامانه‌های اطلاعاتی بین المللی[2]

کنسرسیوم تأیید امنیتیسامانه‌های اطلاعاتی بین‌المللی، صرف نظر از پیشنهاد تأیید تخصصی امنیتی سامانه‌های اطلاعاتی مجاز در اختیار بیش از ۴۵۰۰۰ متخصص در بیش از ۱۲۰ کشور در سراسر دنیا بوده که به‌عنوان مرجع، راهنمایی‌هایی را در صفحات شبکهٔ مجازی خود ارائه می‌کند. متخصصان مجاز نیز برای حفظ اعتبارخود مستلزم احراز هویت واحدهای آموزشی تخصصی خود هستند [۱۴].

۳-۳- سازمان مرجع امنیت اطلاعاتی[3]

مرجع امنیت اطلاعاتی، سازمانی است که اعضای آن بیش از پنجاه درصد از صددرصد یک شرکت مالی را تشکیل می‌دهند. برخی از گزارش‌های توجیهی مرجع امنیت

[1] safe and fair

[2] ISC2:InternationalInformation Systems Security Certification Consortium

[3] ISF:Information Security Forum

اطلاعاتی و استانداردهای آنها در تارنمای این سازمان در دسترس عموم قرار دارد. داده‌های ارائه‌شده توسط همکاران امنیت اطلاعات شرکت‌های عضو, رکن اصلی سیاست‌های مرجع امنیت اطلاعاتی و سایر سیاست‌نامه‌های امنیتی جدید است. این مؤسسه به‌طور منظم اسناد خود را در اختیار اعضا قرار می‌دهد.

۴- شبکه‌سازی امنیت اطلاعاتی

در این بخش برخی اقدامات انجام‌شده در زمینهٔ شبکه‌سازی امنیت اطلاعاتی معرفی می‌شود:

۴-۱- پروژهٔ امنیت کاربرد وب آزاد[1]

انجمن پروژهٔ امنیت کاربرد وب آزاد، مستندات امنیتی فنی و غیرفنی، طرح ها و مطالب منتشره در کنفرانس‌هایشان را بر روی وب ارائه می‌کنند. همچنین فعالیت‌های داخلی کم‌هزینه با موضوعات جذاب را سازمان‌دهی کرده و به‌صورت مجازی با انجمن‌های امنیت اطلاعات داخلی همکاری می‌کنند [۱۱].

۴-۲- ارائهٔ خدمات آموزش امنیت[2]

این مؤسسه از ارائه‌کنندگان معروف خدمات آموزش امنیت است و گواهی‌نامه GIAC[3] را اعطا می‌کند و همچنین منابع امنیتی مفید را از طریق تارنما در دسترس تمام انجمن‌های امنیت اطلاعات قرار می‌دهد، این منابع عبارتند از:

- اطلاعات مربوط به رخدادهای امنیتی؛
- گزارش‌های امنیتی معتبر؛
- نمونه‌هایی از سیاست‌های امنیتی مربوط به منابع؛
- چندین خبرنامه که خوانندگان می‌توانند برای دریافت آنها کد اشتراک (با موضوع اخبار امنیتی, آسیب‌پذیری‌ها و اطلاعات محرمانهٔ امنیتی) بگیرند؛
- جلسات آموزشی امنیت برای دریافت گواهینامهٔGIAC از طریق انجمن‌های داخلی.

۴-۳- تارنمای پاول[4]

تارنمای پاول محصولات امنیت اطلاعات، طرح‌ها و مقالات را به‌صورت رایگان از سال ۲۰۰۵ ارائه می‌کند؛ که نه‌تنها محتوای امنیتی معتبر و رایگان را ارائه می‌کند، بلکه ارتباط شبکه‌ای برخط با یک انجمن امنیتی فعال را از طریق کانال IRC و رایانامه برقرار می‌کند [۱۰].

۴-۴- کنفرانس‌های جهانی امنیت فناوری اطلاعات

نمونه‌هایی از انجمن‌های مرتبط با حوزهٔ نظارتی یا فنی مهارتی ارائه شد که همایش‌هایی را با موضوع امنیت اطلاعات برگزار می‌کنند. این همایش‌ها معتبر و در زمینهٔ امنیت اطلاعات می‌باشند و اغلب برگزارکنندگان آن‌ها افراد فعال و بانفوذ در حوزهٔ امنیت اطلاعات هستند.

۴-۴-۱- همایش نظارتی امنیت RSA

هر سال یک همایش امنیت RSA در آمریکا و دیگری در اروپا برگزار می‌شود. شرکت RSA که بخش امنیتی شرکت EMC است، نخستینین همایش را در سال ۱۹۹۱ با موضوع نظارت امنیت اطلاعات و امنیت کارکنان اجرایی برگزار کرد.

۴-۴-۲- همایش بین‌المللی ISACA

مؤسسهٔ ISACA همایش سالانه‌ای با عنوان نظارت اطلاعاتی، بازرسی اطلاعاتی، امنیت اطلاعاتی و موضوعات مدیریت تهدیدات اطلاعاتی با تأکید بر حوزهٔ اجرایی امنیت برگزار می‌کند.

۴-۴-۳- کنگرهٔ جهانی ISF

شرکت‌های عضو ISF می‌توانند در کنگرهٔ سالانه به‌منظور انتقال تازه‌ترین مقالات و تجربیات ISF شرکت کنند.

۴-۴-۴- سازمان بین‌المللی استاندارد[5]

سازمان بین‌المللی استاندارد در سال ۱۹۴۷ تأسیس شد و یک بخش بین‌المللی غیردولتی است که با کمیتهٔ الکترونیک بین‌المللی[6] و اتحادیهٔ ارتباطات بین‌المللی[7] در رابطه با استانداردهای فناوری اطلاعات و ارتباطات همکاری دارد. استانداردهای زیادی در مورد قانون حفاظت از داده‌ها و سامانه‌های رایانه‌ای در برابرسوء استفاده از آن‌ها، تدوین شده است.

وابستگی شدید به فناوری اطلاعات، همراه با افزایش جرایم رایانه‌ای، در کنار سایر فعالیت‌های قانونی، به‌خصوص

[1] OWASP:Open Web Application Security Project
[2] SANS:The largest source for information security training in the world
[3] GIAC :Global Information Assurance Certification
[4] www.Paul.com

[5] ISO: International Organization for Standardization
[6] IEC: International Electro technical Commission
[7] ITU: International Telecommunication Union

در بخش اقتصادی، ضرورت تدوین استانداردهای امنیتی را ایجاب می‌کند. در این رابطهٔ استانداردهای زیادی ازجمله قوانینی با هدف محافظت از سهامداران و سرمایه‌گذاران نسبت به سرمایه‌گذاری‌هایشان، و نسبت به تصمیمات خود در رابطه با سرمایه‌گذاری‌های زیان‌آور و سامانه‌های اقتصادی ضعیف، تدوین شده است.

۵- مجموعه مدون زیرساخت فناوری اطلاعات - ITIL[1]

در دو دههٔ اخیر فعالیت‌های بسیاری در زمینهٔ ایجاد زیرساخت‌های امن در دنیا صورت گرفته و در این رابطه روش‌ها و توصیه‌های گوناگونی ارائه شده است. ازمیان این روش‌ها، ابتکار سازمان OGC[i] انگلستان است. این استاندارد با گذشت حدود بیست سال از نخستین تلاش‌ها، به‌عنوان استاندارد پذیرفته‌شده دردنیا (استاندارد بین‌المللی[2] ۲۰۰۰۰) در مدیریت سرویس‌های فناوری اطلاعات مطرح است. این استاندارد از اواخر دههٔ ۱۹۸۰ به‌عنوان استاندارد غیررسمی جهانی در مدیریت خدمات مطرح [۱۲] و در ابتدا به‌عنوان راهنمایی برای دولت انگلستان ارائه شد و درنهایت به این نتیجه رسیدند که سازمان‌ها می‌توانند از این چارچوب، در تمامی بخش‌های خود ازجمله امنیت اطلاعات، بهره گیرند؛ زیرا تمامی شرکت‌های ارائه‌دهندهٔ خدمات فناوری اطلاعات، آن را به‌عنوان مبنای مشاوره، آموزش و پشتیبانی نرم‌افزاری پذیرفته‌اند. امروزه، این چارچوب، شناخته‌شده و کاربردی جهانی دارد.

آژانس مخابرات و رایانهٔ مرکزی بریتانیا تصمیم گرفت تا راهی برای بهبود کارایی فناوری اطلاعات در تمامی حوزه‌های آن ازجمله امنیت اطلاعات بیابد. در همین راستا گروهی تشکیل شد تا رویکرد جدیدی برای مدیریت فناوری اطلاعات ارائه دهد. نخستین محصول تولیدی این گروه، GITIM نام داشت که همراه با نخستین نسخه مجموعهٔ مدون زیرساخت فناوری اطلاعات ITIL، در سال ۱۹۸۹ تولید شد. بعد از مدتی نسخهٔ دوم آن در سال ۲۰۰۱ وارد عرصه شد. این نسخه شامل هشت کتاب است که کتاب مدیریت امنیت به‌عنوان یکی از موضوعات مطرح در استانداردهای فناوری اطلاعات، شامل ارائهٔ تعاریف و دستورالعمل‌ها و راه‌کارهای امنیتی برای کلیهٔ حوزه‌های فناوری اطلاعات از جمله راه‌کارهای امنیت اطلاعات است. و نسخهٔ سوم آن در سال ۲۰۰۷ ارائه شد. مجموعهٔ مدون زیرساخت فناوری اطلاعات، مجموعه تجارب شرکت‌ها و سازمان‌های مبتنی بر فناوری اطلاعات است و در طول یک جمع‌بندی کلی به یک مدل عملی تبدیل شده است [۱۵]. از جمله مسائلی که در این حوزه مطرح می‌شود، عبارتند از:

- شناسایی و تدوین استانداردها و خط‌مشی‌های امنیتی مورد نیاز در سازمان؛
- استفاده از زیرساخت‌های سخت‌افزاری امن درسازمان؛
- به‌کارگیری سازوکارهای امنیتی مثل محرمانگی، کنترل دسترسی و ... متناسب با سازمان؛
- رعایت نکات مربوط به امنیت فیزیکی کنترل تردد به اتاق سرور، عدم دسترسی به سوئیچ‌ها و ... درحد مطلوب.
- فراهم‌آوردن دانش کافی در زمینهٔ امنیت اطلاعات و چگونگی به‌روزماندن آن در سازمان؛
- رضایت کارکنان از میزان به‌کارگیری راه‌کارهای امنیت اطلاعات درسازمان.

هدف اصلی مدیریت امنیت اطلاعات، اطمینان از امنیت اطلاعات به‌طور نسبی است؛ درحالی‌که هدف اولیهٔ امنیت اطلاعات، محافظت از دارایی‌های اطلاعاتی در برابر ریسک و حفظ ارزش اطلاعات برای سازمان است که درحقیقت همان اطمینان از صحت، یکپارچگی و قابلیت دسترسی به همراه اهدافی از قبیل اعتبار، مسئولیت‌پذیری، عدم انکار و قابلیت اطمینان است.

۵-۲- ایزو ۲۷۰۰۲[3] راه‌کاری در مدیریت امنیت اطلاعات

این استاندارد بین‌المللی برگرفته از استاندارد BS 77993 است که ابتدا توسط مؤسسه انگلیسی استانداردها وضع شده است؛ و راه‌کارهایی را در مدیریت امنیت اطلاعات بیان می‌کند و به‌عنوان پایهٔ مشترک و راه‌کار عملی برای توسعهٔ استانداردهای امنیتی سازمانی و شیوه‌های مدیریتی اثربخش، در نظر گرفته شده است. این استاندارد شامل راه‌کارها و دستورالعمل‌هایی در ده حوزه امنیتی است:

- سیاست‌های امنیتی؛
- سازماندهی امنیت اطلاعات؛
- مدیریت دارایی‌ها؛

[1] ITIL: Information Technology Infrastructure Library
[2] ISO20000
[3] ISO/IEC 27002:2005

- امنیت منابع انسانی؛
- امنیت فیزیکی و محیطی؛
- مدیریت ارتباطات و عملیات؛
- کنترل دسترسی؛
- سامانه‌های کسب اطلاعات؛
- توسعه و نگهداری؛
- مدیریت حوادث امنیت اطلاعات؛
- مدیریت امنیت سازمان؛
- سازگاری.

در این ده حوزهٔ امنیتی حدود ۳۹ هدف کنترلی و صدها معیار و شیوهٔ کنترل امنیت اطلاعات برای سازمان‌ها توصیه شده است تا دست‌یابی به اهداف کنترلی و محافظت از دارایی‌های اطلاعاتی در مقابل تهدیدات در مقابل محرمانگی، یک‌پارچگی و دردسترس‌بودن اطلاعات مهیا شود [۱].

۵-۳- ایزو[1] ۲۷۰۰۱ الزامات سامانهٔ مدیریت امنیت اطلاعات

استاندارد بین‌المللی ایزو ۲۷۰۰۱ ریشه در اصول فنی بیان‌شده در قسمت دوم استاندارد BS 7799 دارد. این استاندارد به‌طور مشخص الزامات ایجاد، پیاده‌سازی، مانیتورینگ، بررسی، نگهداری و بهبود سامانهٔ مدیریت امنیت اطلاعات[2] در سازمان را بیان می‌کند. این استاندارد برای اطمینان از انتخاب کنترل‌های امنیتی مناسب برای محافظت از دارایی‌های اطلاعاتی طراحی شده است و به‌طورمعمول در انواع سازمان‌ها قابل اجراست. این استاندارد یک مدل چرخه‌ای با عنوان مدل " طراحی، پیاده‌سازی، آزمایش، اجرا"[3] با هدف ایجاد، اجرا، مانیتور و بهبود تأثیر سامانهٔ مدیریت امنیت اطلاعات در سازمان معرفی می‌کند. این چرخه شامل چهار مرحله است:

- طراحی: ایجاد و طراحی سامانهٔ مدیریت امنیت اطلاعات
- پیاده‌سازی: عملیاتی‌کردن سامانهٔ مدیریت امنیت اطلاعات
- آزمایش: مانیتورینگ و بررسی سامانهٔ مدیریت امنیت اطلاعات
- اجرا: نگهداری و بهبود سامانهٔ مدیریت امنیت اطلاعات

اغلب، ایزو ۲۷۰۰۱ همراه با ایزو ۲۷۰۰۲ به‌کار گرفته می‌شود. ایزو ۲۷۰۰۱ الزامات سامانه مدیریت امنیت اطلاعات را تعیین و از ایزو ۲۷۰۰۲ برای مشخص‌کردن مناسب ترین کنترل‌های امنیت اطلاعات در سامانهٔ امنیت اطلاعات استفاده می‌کند. ایزو ۲۷۰۰۲ تجربهٔ عملی در ارائهٔ برخی کنترل‌ها است که سازمان می‌تواند برای رسیدگی به مخاطرات مربوط به امنیت اطلاعات اتخاذ کند. این کنترل‌ها اجباری نیست و این استاندارد گواهی‌نامه هم ندارد؛ اما اگر سازمانی استانداردهای سامانهٔ مدیریت امنیت اطلاعات را به‌کار گیرد، می‌تواند گواهی‌نامه ایزو ۲۷۰۰۱ را کسب کند. فهرستی از نهادهای معتبر که به سازمان‌ها گواهی‌نامهٔ سامانهٔ مدیریت امنیت اطلاعات اعطا می‌کند، در تارنمای ارائهٔ گواهی‌نامهٔ انگلستان وجود دارد [۱۶].

۵-۴- استاندارد BS 7799[4]

این استاندارد نخستین استاندارد مدیریت امنیت است که توسط مؤسسه استاندارد انگلیس ارائه شده است. نسخهٔ نخست این استاندارد در سال ۱۹۹۵ و در یک بخش با عنوان تجربه‌ای در مدیریت امنیت اطلاعات[5] منتشر شد و نسخه دوم آن که در سال ۱۹۹۹ ارائه شد، علاوه بر تغییر نسبت به نسخهٔ نخست، به‌صورت دو بخش مستقل ارائه شد. هدف از تدوین این استاندارد، ارائهٔ پیشنهادهایی در زمینهٔ مدیریت امنیت اطلاعات برای کسانی است که مسئول طراحی، پیاده‌سازی یا پشتیبانی مسائل امنیتی در یک سازمان هستند، بود. این استاندارد متشکل از ۳۵ هدف امنیتی و ۱۲۷ اقدام بازدارنده برای تأمین اهداف تعیین‌شده است که جزئیات و چگونگی انجام آن‌ها را مطرح نمی‌کند؛ بلکه سرفصل‌ها و موضوعات کلی را بیان می‌کند. طراحان این استاندارد معتقدند که در تدوین این استاندارد، ممکن است کنترل‌ها و راه‌کارهای مطرح‌شده در آن برای همهٔ سازمان‌ها قابل استفاده نباشد و یا نیاز به کنترل‌های بیشتری باشد که این استاندارد، آنها را پوشش نداده است. در سال ۲۰۰۰میلادی بخش نخست این استاندارد بدون هیچ‌گونه تغییری توسط مؤسسه بین‌المللی استاندارد، به‌عنوان استاندارد ایزو ۱۷۷۹۹ منتشر شد. و شامل سرفصل‌های ذیل است:

- تدوین سیاست‌های امنیتی سازمان؛
- تشکیلات امنیتی؛
- طبقه‌بندی سرمایه‌ها و تعیین کنترل‌های لازم؛

[1] ISO/IEC 27001:2005
[2] ISMS: Information Security Management System
[3] PDCA=Plan-Do-Check-Act
[4] BS7799
[5] BS7799-1: Code of Practice for Information Security Management

- امنیت کارکنان؛
- امنیت فیزیکی و پیرامونی؛
- مدیریت ارتباطات و بهره‌برداری؛
- کنترل دسترسی؛
- توسعه و پشتیبانی سامانه‌ها؛
- مدیریت تداوم فعالیت؛
- سازگاری.

پس از آن این استاندارد دو بار در سال ۲۰۰۲ میلادی و در سال ۲۰۰۵ بازنویسی و در یک سند منتشر شد. این نسخه متشکل از ۳۹ هدف امنیتی و ۱۳۴ اقدام بازدارنده است [۱۶].

۵-۵- گزارش فنی ایزو ۱۳۳۳۵[1]

مؤسسه استانداردهای امنیت اطلاعات، دارای یک کمیتهٔ فنی مشترک است که کار اصلی آن تهیهٔ استانداردهای بین‌المللی است. این کمیته در مواردی به‌جای تهیه و تدوین یک استاندارد، یک گزارش فنی منتشر می‌کند. گزارش فنی ایزو ۱۳۳۳۵ در قالب پنج بخش مستقل توسط این کمیته تهیه شده و شامل مستندات فنی معتبر است. این گزارش درواقع مکمل استانداردهای مدیریتی ایزو ۱۷۷۹۹ و BS7799 محسوب شده و در پیاده‌سازی سامانهٔ مدیریت امنیت اطلاعات، کاربرد زیادی دارد [۱۷]. این استاندارد شامل مجموعه‌ای از راه‌کارهاست که برای ارزیابی کنترل امنیت فنی به‌کار می‌رود:

- ایزو ۲۰۰۴: ۱-۱۳۳۳۵[2] مستندسازی ابعاد و مدل‌های مدیریت امنیت فنی ارتباطات و اطلاعات را تحت پوشش قرار می‌دهد.
- ایزو ۱۹۹۸: ۳-۱۳۳۳۵[3] مستندسازی فنون مدیریت امنیت فناوری اطلاعات را تحت پوشش قرار می‌دهد.
- ایزو ۲۰۰۰: ۴-۱۳۳۳۵[4] گلچینی از مسائل حفاظتی را پوشش می‌دهد؛ مثل کنترل‌های امنیت فنی.
- ایزو ۲۰۰۱: ۵-۱۳۳۳۵[5] راهنمایی است بر مدیریت امنیت شبکه.

گواهی‌نامه‌های صادرشده در کل دنیا در زمینهٔ امنیت اطلاعات بر اساس استاندارد BS7799 تا تاریخ ۲۰۰۶ به تعداد ۲۵۴۶ عدد است که به‌علت اهمیت این مقوله به‌سرعت در حال افزایش است.

[1] ISO/IEC TR 13335
[2] ISO/IEC 13335-1:2004
[3] ISO/IEC TR 13335-3:1998
[4] ISO/IEC TR 13335-4:2000
[5] ISO/IEC TR 13335-5: 2001

۵-۶- ایزو ۱۵۴۰۸[6] معیارهای ارزیابی امنیت فناوری اطلاعات

استاندارد بین‌المللی ایزو ۱۵۴۰۸ به‌عنوان معیارهای عمومی[7] ارزیابی امنیت فناوری اطلاعات شناخته‌شده که این استاندارد شامل سه بخش است:

- مقدمه و مدل عمومی[8]؛
- الزامات عملکردی[9]؛
- الزامات ضمانتی[10].

این استاندارد کمک می‌کند به ارزیابی، اعتبارسنجی و گواهی تضمین امنیت یک محصول فناورانه در مقابل برخی فاکتورها مثل الزامات عملکردی امنیتی مشخص‌شده در این استاندارد.

سامانه‌ها و محصولات سخت‌افزاری و نرم‌افزاری از لحاظ معیارهای عمومی در آزمایشگاه‌های ارزیابی سطح اطمینان[11] ارزیابی می‌شوند.ارزیابی سطح اطمینان شامل هفت مرحله است:

- آزمایش عملکرد؛
- آزمایش ساختاری؛
- آزمایش متد و بررسی؛
- طراحی روش، بررسی و بازبینی؛
- طراحی و آزمایش نیمه‌رسمی؛
- تأیید و طراحی و آزمایش نیمه‌رسمی؛
- تأیید و طراحی و آزمایش رسمی.

۵-۷- استاندارد امنیت اطلاعات صنعت کارت‌های پرداخت الکترونیکی[12]

این استاندارد شامل دوازده اصل از جمله مدیریت امنیت، سیاست‌ها، رویه‌ها، معماری شبکه، طراحی نرم‌افزار و سایر اقدامات حیاتی است.این الزامات به‌صورت زیر دسته‌بندی شده است:

- ایجاد و نگهداری شبکه امن و پایدار؛
- محافظت از اطلاعات صاحب کارت؛
- ارائهٔ برنامه‌ای برای مدیریت آسیب‌پذیری؛

[6] ISO/IEC 15408
[7] common criteria
[8] ISO/IEC 15408-1:2005
[9] ISO/IEC 15408-2:2005
[10] ISO/IEC 15408-3:2005
[11] EAL: Evaluation Assurance Level
[12] PCIDSS: Payment Card Industry Data Security Standard

- اجرای اقدامات کنترلی قوی در زمینه سطح دسترسی به اطلاعات؛
- نظارت مستمر و آزمایش شبکه؛
- اجرای سیاست‌های امنیت اطلاعات.

۵-۷-۱- برخی مقررات مرتبط با امنیت اطلاعات

علاوه‌بر راه‌کارها و استانداردهای مختلف، برخی سازمان‌ها و شرکت‌ها مثل بانک‌ها، نیاز به یک‌سری مقررات و راه‌کارهایی دارند که متناسب با سیاست‌های کاری خودشان باشد. در این بخش به‌طور مختصر مقررات مورد استفاده در امریکا در رابطه با امنیت اطلاعات را بیان می‌کنیم. آشنایی با این‌گونه مقررات که به‌طور اخص در سایر کشورها مورد استفاده قرار می‌گیرد، تنها بدین جهت است تا بتوانیم برای ارائه و برنامه‌ریزی چنین مقررات و راه‌کارهایی برای کشور خود از آنها ایده گرفته و بتوانیم قوانینی متناسب با نیاز سازمانی خود تدوین و اجرا کنیم [۱۹].

۵-۷-۲- قانون ساربنز ۲۰۰۲ [1]

این قانون در سال ۲۰۰۲ به اجرا گذاشته شد و هدف از آن حمایت از سرمایه‌گذاران برای بهبود بخشیدن به‌دقت و قابلیت اطمینان شرکت‌های بزرگ است که به‌موجب قوانین اوراق بهادار و با اهداف مختلف ایجاد شده‌اند.

در بخش ۴۰۴ این قانون، همان‌گونه که فناوری اطلاعات نقش مهمی را در فرایند گزارش‌های مالی ایفا می‌کند، کنترل‌های فناوری اطلاعات به‌منظور رضایت‌مندی کامل از ملزومات این قانون است. اگر چه ملزومات مربوط به امنیت اطلاعات به‌طور مستقیم در این قانون نیامده است؛ ولی سامانه‌های مالی به هر حال باید اطلاعات قابل اطمینان از طریق ممانعت از تراکنش‌های غیر مجاز ممکن و انباشتگی اعداد و ارقام فارغ از هرگونه اقدامات امنیتی مناسب ارائه دهند. ملزومات این قانون به‌منظور کنترل‌های امنیت اطلاعات سامانه‌ها به‌طور غیر مستقیم با مدیریت سازمان سروکار دارد [۱۸].

۵-۷-۳- قانون بیمهٔ سلامت [2]

این قانون در سال ۱۹۹۶ در امریکا به اجرا گذاشته شد؛ که در آن استانداردهای امنیتی مربوط به اطلاعات سلامت افراد تعریف شده و فاکتورهایی را ازجمله قابلیت‌های فنی، سامانه‌های ثبت اطلاعات به‌منظور حفظ و نگهداری اطلاعات مربوط به سلامت افراد، هزینهٔ اقدامات امنیتی، نیاز به آموزش کارکنان و... مد نظر قرار می‌دهد.

۵-۸- قانون مدیریت امنیت اطلاعات [3]

قانون مدیریت امنیت اطلاعات که بخشی از مقررات مربوط به "دولت الکترونیک" است در سال ۲۰۰۲ تبدیل به قانون شد. آژانس‌های فدرال امریکا موظف به توسعه و اجرای یک برنامه گسترده برای ارائه به آژانس هستند. درواقع ارائهٔ یک چهارچوب امنیت اطلاعات برای اطلاعات و سامانه‌های اطلاعاتی به‌منظور پشتیبانی از اقدامات و دارایی‌های آژانس. برخی از ملزومات آن عبارتند از:

- بررسی دوره‌ای ریسک‌های اطلاعاتی و سامانه‌های اطلاعاتی که ازملزومات و دارایی‌های سازمان پشتیبانی می‌کند [۲۰]؛
- طراحی رویه‌ها و سیاست‌های مبتنی بر ریسک به‌منظور کاهش ریسک‌های امنیت اطلاعات تا سطح قابل قبول؛
- ارائهٔ راه‌کارهایی برای اجرای امنیت مناسب سامانه‌ها و شبکه‌های اطلاعاتی؛
- آموزش‌های آگاهی‌بخشی امنیتی به کارکنان ازجمله پیمان‌کاران؛
- آزمایش و ارزیابی دوره‌ای اثربخشی کنترل‌ها، رویه‌ها و سیاست‌های امنیتی؛ که این ارزیابی دوره‌ای باید حداقل سالی یک‌بار صورت گیرد؛ و انجام اقدامات اصلاحی مناسب برای هریک از نقایص به‌وجود آمده؛
- استفاده از حوادث امنیتی آزمایش‌شده؛
- ارائهٔ طرح پایدار کسب و کار برای پشتیبانی از سازمان.

این استاندارد شامل هفده حوزهٔ امنیتی است:

- کنترل دسترسی ۲- آموزش و آگاهی‌بخشی ۳- ممیزی و پاسخ‌گویی ۴- صدور گواهی‌نامهٔ ارزیابی و اعتباربخشی ۵- مدیریت پیکربندی ۶- برنامه‌ریزی حوادث احتمالی ۷- شناسایی و تصدیق امنیت ۸- واکنش در مقابل حادثه ۹- نگهداری ۱۰- حفاظت رسانه‌ای ۱۱- حفاظت فیزیکی و پیرامونی ۱۲- برنامه‌ریزی ۱۳- امنیت کارکنان ۱۴- ارزیابی ریسک

[1] SOX :Sarbanes- Oxley Act of 2002

[2] HIPPA: The Health Insurance Portability And Accountability Act

[3] FISMA: Federal Information Security Management Act

۱۵- کسب خدمات و سامانه‌ها ۱۶- حفاظت ارتباطات ۱۷- یک‌پارچگی اطلاعات و سامانه‌ها [۲].

۵-۸-۱- استانداردهای پردازش اطلاعات دولت فدرال[1]

این استاندارد از سری استانداردهای منتشرشدهٔ مؤسسهٔ ملی فناوری و استانداردها است که مربوط به راه‌کارها و استانداردهای اتخاذشده در ذیل مفاد قانون مدیریت امنیت اطلاعات فدرال است.

گرچه استانداردهای امنیتی زیادی در دسترس هستند؛ ولی همهٔ آن‌ها استانداردهای عمومی هستند که نمی‌تواند برای همهٔ سازمان‌ها و یا سازمان خاصی مورد استفاده قرار گیرد. اگر سازمانی بخواهد کنترل‌های امنیتی را که در ارتباط با استاندارد خاصی است، اجرا کند، باید تلاشی هماهنگ از مدیریت سازمان گرفته تا مصرف‌کنندهٔ نهایی در این فرایند انجام گیرد. سازمان ابتدا باید یک تجزیه تحلیل شکاف[2] انجام دهد تا بتواند کنترل‌های امنیتی موجود در سازمان، مسائل و مشکلات بالقوه، هزینه و سود، تأثیر عملیاتی و نظریه‌های پیشنهادی را قبل از اتخاذ هرگونه استانداردی شناسایی کند. ایجاد سیاست‌ها و راه‌کارهای امنیتی، می‌بایست فقط به‌دنبال تحلیل شکاف انجام گیرد و پشتیبانی مدیریت در کلیهٔ مراحل لازم و ضروری است. برنامه‌های آگاهی‌بخشی کاربران نیز به‌منظور اطمینان‌دادن به کلیهٔ کارکنان از منافع و تأثیرات این راه‌کارها و سیاست‌های امنیتی جدید در دستور کار قرار می گیرد.

مشکل عمومی که بعد از به‌اجراگذاشتن هر استانداردی به‌وجود می‌آید، افزایش شکایات کاربران سرویس‌های فناوری اطلاعات است که به‌خاطر محدودیت‌های به‌وجودآمده در اثر اعمال کنترل‌های امنیتی جدید به‌وجود می‌آید. برای اجرای موفق هرگونه استاندارد امنیت اطلاعات می‌بایست بین ملزومات امنیتی، ملزومات عملیاتی و ملزومات کاربر تعادل به‌وجود بیاید. امنیت چیزی است که باید تمامی گروه‌های سازمانی در آن سهیم باشند. مدیریت ارشد،کارکنان امنیت اطلاعات،کاربران و متخصصان فناوری اطلاعات همگی در تأمین امنیت دارایی‌های سازمان دارای یک نقش مشترک هستند. موفقیت امنیت اطلاعات فقط از طریق همکاری و مشارکت کامل کلیهٔ سطوح سازمانی، هم در خارج و هم در داخل سازمان امکان‌پذیر می‌شود [۲۱].

[1] FIPS :The Federal Information Processing Standards
[2] gap analysis

۵-۹- سامانهٔ مدیریت امنیت اطلاعات[3]

سامانه مدیریت امنیت اطلاعات مبتنی بر مدل چرخه‌ای، طراحی، پیاده‌سازی، آزمایش، اجرا[4] است؛ و کنترل‌های امنیتی استاندارد BS7799 را پیاده‌سازی می کند. مراحل هشت‌گانهٔ ایجاد سامانه مدیریت امنیت اطلاعات:

۵-۹-۱- تعیین و تعریف محدوده عملیاتی[5]

این محدوده می‌تواند شامل مشخصات فعالیت‌های تجاری و کاری، سازمانی، محل‌های مورد نظر آن، دارایی‌ها و فناوری‌های سازمان باشد.

۵-۹-۲- تعریف و تدوین سیاست سامانه مدیریت امنیت اطلاعات

۱. شامل چارچوبی برای تنظیم اهداف سازمان و پی‌ریزی و استخراج قواعد کلی و دستورالعمل‌های امنیتی جهت حفاظت از اطلاعات سازمان؛
۲. لحاظ‌نمودن نیازهای کاری و قانونی و الزامات امنیتی؛
۳. ایجاد بخشی به نام مدیریت ریسک و تشکیلات امنیت سازمانی جهت استقرار و پشتیبانی سامانهٔ مدیریت امنیت اطلاعات؛
۴. ایجاد معیاری جهت برآورد میزان ریسک و مقابله با آن؛
۵. تدوین، گردآوری و تصویب سند سیاست سامانه مدیریت امنیت اطلاعات؛

۵-۹-۳- تعریف رویکرد سیستمی برای برآورد میزان ریسک

تعریف روشی برای ارزیابی میزان مخاطره، متناسب و مرتبط با سامانه مدیریت امنیت اطلاعات و تعیین امنیت اطلاعات کاری و تجاری، الزامات انظباطی و قانونی، تنظیم اهداف و سیاست‌های سامانه مدیریت امنیت اطلاعات در راستای کاهش میزان مخاطرات به سطح قابل قبول.

۵-۹-۴- تعیین مخاطرات

۱. تعیین دارایی‌های داخل محدوده عملیاتی و مالکان مربوطه؛
۲. تعیین تهدیدات موجود علیه دارایی‌ها؛
۳. تعیین نقاط آسیب‌پذیری که ممکن است توسط تهدیدات امنیتی مورد سوء استفاده و نفوذ قرار گیرند؛

[3] ISMS: Information security Management system
[4] PDCA=Plan-Do-Check-Act
[5] ISMS scope

۴. تعیین صدماتی که باعث خدشه یا از دست رفتن پارامترهای مهم امنیتی نظیر محرمانگی، صحت و یک‌پارچگی و در دسترس بودن اطلاعات می‌شود.

۵-۹-۵- برآورد میزان مخاطرات

- برآورد زیان‌های کاری ناشی از یک اشکال و خطای امنیتی؛ در این امر بایستی پیامدهای احتمالی ناشی ازدست‌رفتن محرمانگی، یک‌پارچگی و دردسترس بودن دارایی‌ها را مد نظر قرار داد.
- برآورد واقع‌گرایانه احتمال وقوع اشکال امنیتی که به سبب تهدیدات و آسیب‌پذیری‌های متداول رخ می‌دهد و همچنین برآورد تأثیراتی که بر این دارایی‌ها گذاشته و کنترل‌هایی که در حال حاضر اعمال می‌شود؛
- تخمین سطوح مخاطرات؛
- تعیین مخاطرات قابل قبول یا نحوهٔ مقابله و برخورد با آنها با استفاده از معیار به‌دست‌آمده؛

۵-۹-۶- شناسایی و ارزیابی حالت‌های مختلف مقابله با مخاطرات

فعالیت‌های ممکنه عبارتند از:

- اعمال کنترل‌های مناسب؛
- قبول هدفمند و عمدی مخاطرات به شرط آن‌که، این مخاطرات به‌وضوح سیاست‌ها و معیارهای سازمان در زمینهٔ پذیرش مخاطره را برآورده کند؛
- اجتناب و پرهیز از مخاطرات؛
- واگذاری خسارات احتمالی مخاطرات اجتناب ناپذیر سازمان به طرف‌های دیگر، مانند شرکت‌های بیمه؛

۵-۹-۷- گزینش اهداف کنترلی و کنترل‌های مربوط به مقابله با مخاطرات

اهداف کنترلی و کنترل‌ها، بایستی از این استاندارد انتخاب شوند و این گزینش بایستی براساس نتیجه‌گیری‌های حاصله از فرآیند تشخیص و نحوهٔ مقابله با مخاطره توجیه شود [۲۱].

نکته: اهداف کنترلی و کنترل‌های فهرست‌شده در این استاندارد جامع و کامل نیستند و می‌توان اهداف کنترلی و کنترل‌های دیگری به آن اضافه کرد.

۵-۹-۸- تهیه بیانیهٔ کاربردی و عملی

اهداف کنترلی و کنترل‌های ذکرشده و دلایل انتخاب آنها بایستی در بیانیهٔ مذکور ذکر شود؛ همچنین هرگونه استثنای اهداف کنترلی و کنترل‌های فهرست‌شده نیز باید در آن به ثبت برسد.

۵-۱۰- مدیریت ریسک فناوری اطلاعات

در پژوهشی که توسط جانر و کرمر(۲۰۰۵)[1] انجام شده، به‌منظور کاهش ریسک‌های فناوری اطلاعات، یک چهارچوب تئوریک برای تحلیل ایجاد فرهنگ ریسک ارائه دادند. امنیت اطلاعات و مدیریت امنیت فناوری اطلاعات اجزای کلی مدیریت ریسک فناوری اطلاعات هستند. Jahner و Krcmar با استفاده از تجربیات خود فاکتورهای مهمی را برای اجرای فرهنگ ریسک به‌دست آوردند از جمله گروه‌های ارتباطی یا دخالت‌دادن مدیریت ارشد سازمان در بحث مدیریت ریسک (شکل ۱).

۵-۱۱- آگاهی امنیتی

انجمن امنیت اطلاعات امریکا[1]، آگاهی امنیتی را این‌چنین تعریف می‌کند: میزان فهم و دانش هر یک از رؤسای سازمان نسبت به موارد زیر:

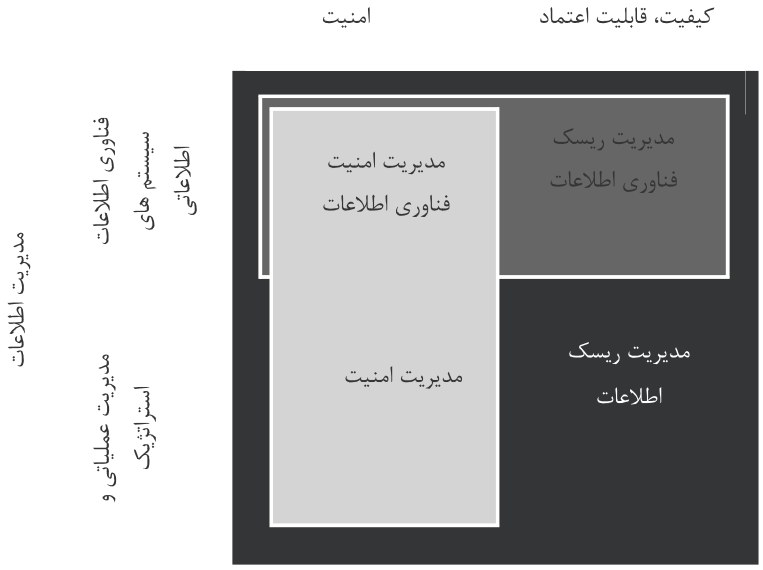
- میزان درک و آگاهی از اهمیت امنیت فناوری اطلاعات؛
- میزان درک و آگاهی از سطوح امنیت فناوری اطلاعات متناسب با سازمان.
- میزان درک و آگاهی از تعهدات و وظایف امنیتی خود، و این‌که آیا مطابق آن‌ها عمل می‌کنند.

۵-۱۲- مدیریت امنیت فناوری اطلاعات و سازمان‌دهی امنیت اطلاعات

استانداردها، چهارچوب‌ها و مدل‌های فراوانی برای مدیریت امنیت اطلاعات وجود دارد. در همین اواخر سازمان‌ها چهارچوب‌هایی را که خود تدوین کرده‌اند، استفاده می‌کنند و معتقدند که استفاده از این استانداردها و به‌کارگیری ملزومات خاص سازمان، خود می‌تواند بیشترین تأثیر را در

[1] ISF: Information Security Forum

برقراری امنیت اطلاعات در سازمان داشته باشد. در یکی از پژوهش‌های انجام‌شده در این زمینه، نشان داده سازمان‌هایی که بر اساس استاندارد BS7799-2 کار کرده‌اند، به رشد و بلوغ سازمانی بالاتری نسبت به سازمان‌هایی که به‌طور غیر رسمی سعی در برقراری امنیت اطلاعات خود کرده‌اند، دست یافته‌اند.

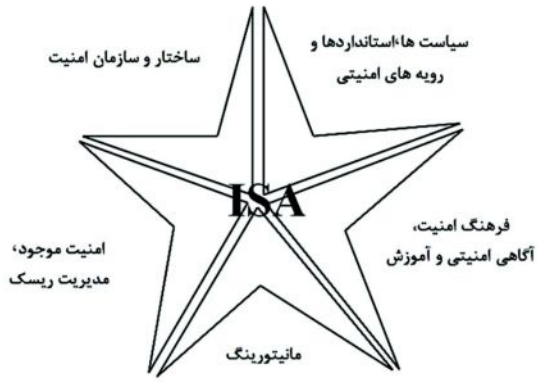


(شکل- ۱) : مدیریت ریسک

۵-۱۲-۱- معماری امنیت اطلاعات و مدیریت امنیت اطلاعات

مفهوم معماری امنیت اطلاعات توسط خانم *کیلمایر* در سال ۲۰۰۰ بیان شد، این معماری امنیت شامل فرایند توسعه دانش ریسک، ارزیابی کنترل‌های موجود و بالاخره هم‌سان‌سازی کنترل‌های موجود و جدید برای دست‌یابی به الزامات امنیت اطلاعات سازمان است [۲۲].

معماری امنیت اطلاعات چیزی نیست که بتوانیم آن را خریداری کنیم [۲۳]. او چهارچوبی را برای معماری امنیت اطلاعات ارائه داده است. شکل(۲)



(شکل- ۲): معماری امنیت اطلاعات

۵-۱۳- همایش‌های فنی

همه‌ساله در زمینهٔ امنیت اطلاعات، همایش‌هایی به‌منظور بررسی ابعاد مختلف امنیت و ارائهٔ راه‌کارها و تبادل تجربیات سایر کشورها در حوزهٔ امنیت برگزار می‌شود. در زیر به معرفی برخی از معروف‌ترین این همایش‌ها در سطح بین‌الملل می‌پردازیم.

۵-۱۳-۱- همایش دفکن هکینگ[52]

این همایش یکی از شناخته شده ترین همایش‌ها با موضوع هک با مشارکت فعالان حوزهٔ امنیت فنی است. این همایش توسط جف ماس در سال ۱۹۹۳ برگزار شد و در سال ۲۰۰۹ بیش از ده هزار شرکت‌کننده داشت. این همایش در فصل تابستان و در لاس‌وگاس برگزار می‌شود و به‌طور معمول آسیب‌پذیری‌های شناخته‌شده

[52] Defcon Hacking

امنیتی در طول همایش بین افراد متخصص مورد تبادل نظر قرار می‌گیرد. موضوعات مطرح‌شده در همایش به اختصار جهت اطلاع‌رسانی به متخصصانی که موفق به حضور در همایش نمی‌شوند در تارنمای همایش یا سایر سایت های مربوط به امنیت اطلاعات منتشر می شود [۲۳].

۵-۱۳-۲- کنفرانس کلاه سیاه[۵۳]

این کنفرانس شامل یک سری همایش‌هایی است که هر سال در چند مکان مختلف برگزار می‌شوند. این همایش نیز توسط جف ماس در سال ۱۹۹۷برگزار شد و سپس امتیاز این همایش را در سال ۲۰۰۵ به فروش رساند. این همایش‌ها به موضوعاتی امنیت فنی، به‌طور تخصصی‌تر توجه دارند. هزینهٔ اولیهٔ این همایش به‌طور قابل توجهی بسیار بیشتر از هزینهٔ برگزاری همایش Defcon است. درنتیجه تعداد شرکت‌کنندگان این همایش کمتر است.

۵-۱۳-۳- مؤسسهٔ او دبلیو ای اس پی[۵۴]

اکثر شعب داخلی این مؤسسه هر سال حداقل یک همایش نیم‌روزه یا یک‌روزه را برگزار می‌کنند. غیر از همایش‌های داخلی، همایش‌های جهانی با موضوع امنیت برنامهٔ کاربردی رانیز در آمریکا برگزار می‌کنند. این مؤسسه اطلاعات مربوط به همایش‌ها را در سایت خود ارائه می‌کند [۲۵].

۵-۱۳-۴- همایش کن سی وست[۵۵]

این همایش سالانه و در ونکوور(کانادا) برگزار می‌شود که مسائلی در مورد امنیت فنی در آن مطرح می‌شود. برخی از موضوعات آن از سایت همایش قابل اقتباس است.

۵-۱۳-۵- همایش شیمو کن[۵۶]

همایشی با موضوع هک که در ساحل شرقی آمریکا و به شکل غیر رسمی برگزار می‌شود و بلیط شرکت در این همایش به‌صورت شگفت‌آوری به فروش می‌رسد و رقابت برای شرکت در آن بسیار است.

۵-۱۳-۶- همایش بورکن[۵۷]

این همایش, همایشی نو در بعد فنی امنیت اطلاعات است که در سال ۲۰۰۹ در بروسل آغاز شد و یک اقدام اروپایی است که از طریقاین همایش بین کارآموزان امنیتی ارتباط شبکه ای ایجاد می‌کند.

در کنار این اسامی شناخته‌شده، همایش‌ها و برنامه‌های کوچک‌تری نیز برگزار می‌شوند که تعداد آنها در حال افزایش است؛ و این همایش‌ها به شکل‌های مختلف و توسط انجمن‌های امنیتی داخلی برگزار می‌شوند.

۶- مقررات و دستورالعمل‌های مربوط به امنیت فناوری اطلاعات در داخل کشور

بحث امنیت اطلاعات در سال‌های اخیر توجه مسئولان کشور را به خود جلب کرده که در این رابطه همایش‌ها و کنفرانس‌هایی درخصوص این موضوع برگزار شده است؛ همچنین مقررات و دستورالعمل‌هایی نیز در این رابطه تدوین و جهت اجرا به دستگاه‌های دولتی ابلاغ شده است. در زیر به عناوین برخی از این قوانین و مقررات اشاره می‌شود:

۲۴-۱ "سند راهبردی جامعه اطلاعاتی ایران " شورای عالی اطلاع رسانی، بهمن ۱۳۸۷،

۲۴-۲ "سیاست‌های کلی حوزهٔ فناوری اطلاعات و ارتباطات"، مصوبات مجمع تشخیص مصلحت نظام، ۱۳۸۶.

۲۴-۳ "نظام جامع فناوری اطلاعات کشور (سند راهبردی)"، کمیتهٔ راهبری تدوین نظام جامع فناوری اطلاعات، معاونت فناوری اطلاعات وزارت ارتباطات و فناوری اطلاعات ،۱۳۸۶

۲۴-۴ "سند فرابخشی (ویژه) بهینه‌سازی تشکیلات دولت و دولت الکترونیک"، سازمان مدیریت و برنامه‌ریزی کشور، ۱۳۸۵

۲۴-۵ قانون برنامهٔ پنجسالهٔ پنجم توسعهٔ جمهوری اسلامی ایران (۱۳۹۴ ـ ۱۳۹۰)[۵۸]

۷- نتیجه‌گیری

از مجموع استانداردها و قوانین تدوین‌شدهٔ امنیت اطلاعات در دنیا و اقدامات انجام‌شده در این رابطه، بیش از پیش به اهمیت این مقوله پی می‌بریم و این‌که اهمیت آن در حدی است که در اروپا و امریکا سرمایه‌گذاری‌های کلانی در رابطه

[53] Black Hat Conference
[54] OWASP
[55] CanSeeWest
[56] ShmooCon
[57] Broucon

[۵۸] متن کامل اسناد فوق در سایت اطلاع رسانی وزارت ارتباطات و فناوری اطلاعات در دسترس عموم می باشد. (آدرس:http://www.itc.ir)

با امنیت شبکه و فضای تبادل اطلاعات کرده‌اند؛ به‌طوری‌که در قانون اصلاح پژوهش و توسعهٔ امنیت شبکه‌ای سال ۲۰۰۹ در آمریکا، اعتباری به مبلغ هفت میلیون دلار در سال ۲۰۱۰ و افزایش این رقم به نود میلیون دلار تا سال ۲۰۱۴ برای پژوهش در زمینهٔ امنیت شبکه و سامانه‌های رایانه‌ای به تصویب رسید و همچنین اتحادیهٔ اروپا بودجه‌ای به مبلغ ۷.۹۳ میلیون یورو به آژانس امنیت شبکه و اطلاعات اروپا (ENISA) برای سال ۲۰۰۹ اختصاص داد. با توجه به موارد بالا و تهدیدهای بسیاری که پیش روی سازمان‌ها قرار دارد، لازم است مسئولان توجه جدی‌تری به مقولهٔ امنیت اطلاعات داشته، و استراتژی خود را بر پایهٔ سرمایه‌گذاری بر روی امنیت اطلاعات سازمان بنا نهند و آن را با محافظت از موجودیت سازمان در هم آمیخته و تخصیص منابع مالی برای آن را هزینه نداشته، بلکه آن را سرمایه‌گذاری بدانیم.

در پایان یادآوری می‌شود با توجه به این‌که مقولهٔ امنیت اطلاعات در سازمان‌ها اهمیت بالایی دارد، لذا محدودیت در انجام مطالعهٔ موردی سازمان و یا شرکت خاص امکان‌پذیر نبوده و اغلب سازمان‌ها تمایل به ارائه اطلاعاتی در این زمینه ندارند. و به‌یقین دستورالعمل‌ها و سیاست‌گذاری‌های ابلاغی را در این زمینه در دستور کار خود قرار داده‌اند.

۸- منابع

[۱] قانون برنامه پنج ساله پنجم توسعه جمهوری اسلامی ایران (۱۳۹۴ ـ ۱۳۹۰) فصل چهارم، نظام اداری و مدیریت فناوری اطلاعات.

[۲] سعید علوی وفا – علیرضا پورابراهیمی، تهدید شناختی شبکه های اجتماعی در فضای سایبر و تاثیر آن بر تغییر پارادایم های راهبردی، نخستین همایش ملی دفاع سایبری بهمن ۱۳۹۰.

[۳] دکتر علیرضا پور ابراهیمی- دانشجو: مسعود ظهرابی، پایان نامه کارشناسی ارشد: بررسی راهکارهای ورود ITIL به سازمان مبتنی بر استراتژی مدیریت دانش ۱۳۹۰.

[۴] مرضیه شریعتی، پایان نامه کارشناسی ارشد: ارائه یک چارچوب تعامل پذیر معماری امنیت اطلاعات در کاربردهای فرا/درون سازمانی ۱۳۸۹.

[۵] متن کامل سند چشم انداز جمهوری اسلامی ایران در ۱۴۰۴ هجری شمسی.

[۶] مصطفی درزی رامندی، پایان نامه کارشناسی ارشد: ارایه چارچوب توسعه زیرساخت‌های دولت الکترونیک در ایران (چشم انداز ایران ۱۴۰۴) تیرماه ۱۳۸۹.

[7] Partida, A. IT Security Management-IT Securiteers-setting up an IT Security Function, 2010.

[8] Balboni, P., Firm, L. Data Protection and Data Security Issues related to Cloud Computing in the EU, (Milan-Bologna Italy) / European Privacy Association / Italian Institute for Privacy / Tilburg University, 2010.

[9] The Government of the Hong Kong Special Administrative Region, An Overview of Information Security Standards, February 2008.

[10] Ladan, Sh., Yari, A. and Khodabandeh, H. Combination of Information Security Standards to Cover National Requirements, World Academy of Science, Engineering and Technology, 2006.

[11] Solove, D. J. Data Security and Personal Information, 2008.

[12] Ozcelik, Y. and Rees, J. A New Approach for Information Security Risk Assessment: Value at Risk, May 2005.

[13] Solove, D. J. and Hoofnagle, C. J. A Model Regime of Privacy Protecion, 2006

[14] Munteanu, D., Ioan, A. and Romania, I. Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma, 2009.

[15] Goh, R. Information Security: The Importance of the Human Element/ Presented to the Faculty of the Preston University In partial fulfillment of the requirements for the degree of Doctor of Philosophy in Business Administration by Information Security Classification February *Produced by* Information Management Branch Government and Program Support Services Division Alberta Government Services /Edmonton, Alberta, Canada 2005.

[16] Manar, A.T. and Adel, Kh. Exploratory Study on Innovation Use of ISO Standards for IT Security in the UAE/ European, Mediterranean & Middle Eastern Conference on Information Systems, Athens, Greece, El Barachi May 30-31 2011.

[17] Nordlander, J. A Comparison Between Existing SCADA System Security Standards and ISO 17799/ A Master Thesis, 2009.

[18] Gordon, L.A., Loeb, M. P., Smith, R. H. and Madrid, T. S. The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities, Spain July 20, 2006.

[19] Jean Camp, L. The State of Economics of Information Security, March 9, 2006.

[20] Berends, A.C. Master Thesis on “Dealing with information loss”, 2010.

[21] Cukier, K. N., Mayer-Schönberger, V. and Branscomb, L.M. Ensuring (and Insuring)Critical Information Infrastructure Protection, October 2005.

[22] Carlson, T. Information Security Management: Understanding ISO 17799, 2001.
[23] Implementing Information Security Based on ISO 27001 and ISO 27002/www.alc-group.com
[24] Carlson, T. Information Security Management: Understanding ISO 17799, 2001.
[25] Arraj, V. ITIL: The Basics, White Paper /May 2010.

مینا فیلی مدرک کارشناسی مترجمی زبان انگلیسی را از دانشگاه علامه طباطبایی و کارشناسی ارشد خود را در رشتهٔ مدیریت فناوری اطلاعات از دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران در سال های ۱۳۷۸ و ۱۳۹۰ دریافت کرد. از سال ۱۳۸۳ تاکنون در نهاد ریاست جمهوری اسلامی ایران مشغول به‌کار می‌باشند. زمینهٔ پژوهشی مورد علاقهٔ ایشان استانداردهای امنیت اطلاعات است.

منصور اسماعیل‌پور مدرک کارشناسی و کارشناسی ارشد خود را در رشتهٔ مهندسی کامپیوتر-نرم افزار در سال‌های ۱۳۸۱ و ۱۳۸۳ دریافت کرد. مدرک دکترای خود را در رشته مهندسی کامپیوتر– هوش مصنوعی از دانشگاه ملی مالزی در سال ۲۰۱۲ اخذ و از سال ۲۰۱۲ تا ۲۰۱۴ به عنوان فوق دکتری در همان دانشگاه به تحقیق و پژوهش پرداخت. وی از سال ۱۳۸۱ تاکنون عضو هیات علمی گروه مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد همدان است. زمینهٔ پژوهشی مورد علاقه ایشان داده‌کاوی، فرآیندکاوی، یادگیری ماشین و سیستم‌های یادگیر است.