مدیریت امنیت در سیستم های اطلاعاتی

ابراهیم محمود زاده *
مهدی رادرجبی **

چکیده

هدف اصلی این پژوهش شناسایی و سنجش تاثیر عواملی است که سیستم‌های اطلاعاتی سازمانها را با خطر سرقت، نابودی و یا تغییر اطلاعات مواجه می سازند. به‌منظور تعیین عوامل تاثیرگذار بر امنیت اطلاعات،با مرور پژوهشهای پیشین، روشها و استانداردهای رایج جهان ، پر کاربردترین آنها را که با ساختار سازمانهای کشورمان هماهنگی بیشتری داشت، انتخاب شد و در تدوین چارچوب نظری پژوهش مورد استفاده قرار گرفت.

بر اساس بررسی‌های انجام شده مدلی طراحی شد و مولفه‌ها و شاخصهای کلیدی پژوهش مشخص شدند. امنیت نیروی انسانی، امنیت فیزیکی و امنیت اطلاعات سه اصلی می باشند که اعتبار آن با طراحی و اجرای پرسش‌نامه، مورد سنجش قرار گرفت. نتایج حاصل از پژوهش نشان می‌دهد مولفه عدم آگاهی کاربران بالاترین تهدید و پس از آن امنیت نیروی انسانی دومین تهدید برای امنیت اطلاعات سیستمهای رایانه‌ای می باشد. مولفه های امنیت فیزیکی و امنیت اطلاعات به ترتیب در رتبه‌های بعدی قرار دارند.

مفاهیم کلیدی : امنیت اطلاعات، مدیریت امنیت اطلاعات ، استاندارد های امنیت اطلاعات، روشهای استقرار امنیت اطلاعات.

* استادیار دانشگاه صنعتی مالک اشتر و مدیرعامل شرکت صنایع الکترونیک ایران
** کارشناس ارشد مدیریت مراکز اطلاع رسانی- دانشگاه صنعتی مالک اشتر

مقدمه

از فناوری اطلاعات می‌توان به‌عنوان بزرگ‌ترین فناوری در طول تاریخ یاد کرد که توانسته بین رشته‌های مختلف علوم، ارتباط برقرار کند. این فناوری با بکارگیری تمام علوم توانسته‌است اطلاعات مورد نیاز پژوهشگران، صنعتگران، بازرگانان و همچنین قشرهای مختلف جامعه را در کمترین زمان و بهترین وجه فراهم کند به‌طوری که می‌توان ادعا کرد امروزه فناوری اطلاعات، مرزهای کشورهای مختلف را در نوردیده و ملتها را در یک جامعه جهانی گردهم آورده است.

گفتن و شنیدن از مزایای فناوری اطلاعات و امکاناتی که برای بشر به ارمغان آورده همواره لذت‌بخش است. اما این فناوری همانند سایر فناوری‌ها هم‌چون سکه دو رو دارد: «فرصت» و «تهدید». اگر به همان اندازه که به توسعه و فراگیری آن توجه می‌کنیم به امنیت آن توجه نکنیم می‌تواند به یک تهدید و مصیبت بزرگ تبدیل شود.

حجم بالای اطلاعات در هر سازمان در قالب طرح‌ها، نقشه‌ها، سیاستها، بخشنامه‌ها، مکاتبات بازرگانی، مستندات پروژه‌های پژوهشی و سایر اطلاعاتی که ما برای ذخیره‌سازی و پردازش در اختیار این فناوری قرار می‌دهیم، ما را برآن می دارد تا به فکر حفاظت از آن نیز باشیم. اطلاعات یاد شده مهمترین دارایی و کلید رشد و موفقیت هر سازمان است. اگر ما نتوانیم این دارایی مهم را از دسترس نامحرمان و سایر تهدیدها حفظ کنیم به‌شدت آسیب می‌بینیم.

پژوهشگران بر این باورند که اکثر سازمانها بدون توجه به تهدیدات فناوری اطلاعات، هزینه‌های بسیاری برای توسعه این فناوری صرف می‌کنند و اغلب با اجرای راهبردهای مقطعی (مانند نصب آنتی‌ویروس، دیوار آتش و...) سعی دارند تا سازمان و اطلاعات خود را حفظ کنند. بسیار مشاهده شده سازمان‌ها خسارت شدیدی را از این بابت متحمل شده‌اند، اما متاسفانه همین روش را هم‌چنان ادامه می‌دهند.

ضرورت این پژوهش از آن‌جا احساس می شود که در عصر حاضر سازمانها با ارزش‌ترین دارایی خود را جهت پردازش و ذخیره‌سازی در اختیار تجهیزات فناوری اطلاعات قرار داده‌اند. وابستگی به این فناوری باعث شده است تا اگر در ارایه خدمات خللی پیش آید سازمانها نتوانند به کار خود ادامه دهند. بدین ترتیب حیات سازمانها ارتباط نزدیکی با سیستمهای اطلاعاتی آنها دارد. سیستمهای اطلاعاتی نیز همواره در خطر سرقت اطلاعات، تغییر اطلاعات و ایجاد وقفه در ارایه خدمات می‌باشند. از این‌رو سازمانها برای ایمن ماندن از این آسیبها باید به فکر امنیت اطلاعات باشند.

هدف اصلی از انجام این پژوهش بررسی اجمالی سیستمها و روشهای پیاده‌سازی امنیت

اطلاعات است تا بتوان الگوی مناسبی برای ایمن سازی فضای تبادل اطلاعات سازمان ارایه کرد.

مبانی نظری پژوهش

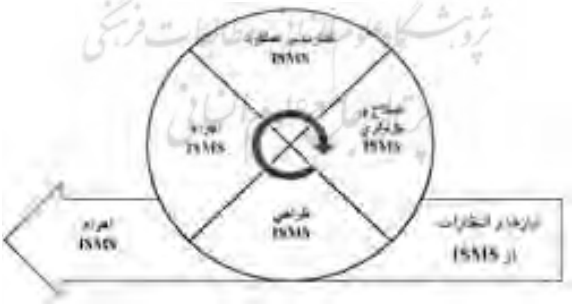
برای محافظت از اطلاعات سازمان نمی‌توان به‌نوع خاصی از امنیت، و یا به یک محصول خاص اکتفا کرد. این که ما انتظار داشته باشیم یک محصول تمام احتیاجات امنیتی ما را برای سیستمهای کامپیوتری و تجهیزات شبکه فراهم کند، رویایی بیش نیست(میوالد،۱۳۸۳). دلیل این ادعا را می‌توان سرعت رشد بسیار سریع فناوری در حوزه فناوری اطلاعات دانست. تجربه نشان داده برخی از محصولات، در زمان عرضه دارای بالاترین سطح ایمنی بوده‌اند، اما در زمان کوتاهی پس از عرضه، روشهایی ابداع شده است که توانسته‌اند به راحتی از موانع امنیتی آنها عبور کنند. سه نمونه از روشهای رایج در جهان که بیشترین کاربرد را در طراحی مدل استقرار امنیت نظامهای اطلاعاتی در سازمانها داشته‌اند مورد بررسی قرار می‌گیرند.

استاندارد BS7799

اولین مرکزی که به‌طور متمرکز اقدام به تهیه معیارهایی برای سنجش امنیت اطلاعات کرد، مرکز امنیت کامپیوترهای تجاری[۱] در کشور انگلستان بود که در سال ۱۹۸۷ میلادی فعالیت خود را آغاز کرد. این مرکز با دو هدف عمده تشکیل شد. اولین هدف تعریف معیارهای بین المللی برای ارزیابی میزان امنیت تجهیزات تولید شده توسط تولیدکنندگان تجهیزات امنیتی و اعطای نشانها و تاییدیه‌های بین المللی به آنها بود و دومین هدف کمک به کاربران جهت انتخاب مناسب تجهیزات مورد نیازشان بود. (British standard institute,1999).

این مرکز در سال ۱۹۸۹ اقدام به انتشار آیین‌نامه‌ای برای سنجش میزان امنیت کرد که به نظامنامه کاربران[۲] معروف شد. مدتی بعد از معرفی این آیین‌نامه، کمیت و کیفیت آن از سوی مرکز محاسبات بین المللی[۳] و یک کنسرسیوم از کاربران که اعضای آن صاحبان صنایع انگلستان بودند، مورد بررسی قرار گرفت و درنهایت به‌عنوان نخستین نسخه استاندارد امنیت با عنوان «مستندات راهبری پی دی ۰۰۰۳» در انگلستان منتشر شد. پس از آن یک گروه کاری ویژه برای امنیت اطلاعات در موسسه استاندارد انگلستان تشکیل شد. این گروه در سال ۱۹۹۲، اولین نتیجه پژوهشهای خود را تحت عنوان آیین‌نامه مدیریت امنیت اطلاعات[۴] منتشر کرد و سه سال بعد یعنی در سال ۱۹۹۵ ، آن موسسه، استاندارد BS۷۷۹۹ را براساس نتایج این پژوهش تدوین و منتشر کرد.

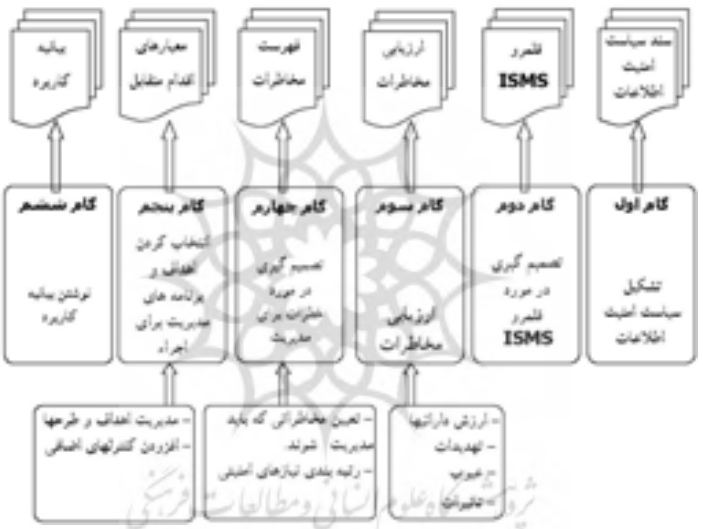
این استاندارد، در دو بخش تدوین شده است:
بخش اول استاندارد، ده حوزه کنترلی را معرفی می کند که یک راهنمای پیاده‌سازی است و از آن می‌توان به‌عنوان ابزاری برای توسعه ساختار مناسب امنیت اطلاعات استفاده کرد. به‌عبارت دیگر به‌عنوان مبنای تشخیص مخاطرات به‌کار می‌روند. ده حوزه کنترلی شامل تدوین سیاست امنیتی، ایجاد تشکیلات تامین امنیت سازمان، طبقه بندی و کنترل دارایی ها، امنیت نیروی انسانی، امنیت فیزیکی و پیرامونی، مدیریت تداوم فعالیت، مدیریت ارتباطات و بهره‌برداری، کنترل دسترسی، سازگاری با قوانین و توسعه و پشتیبانی سیستمها می‌باشد.
بخش دوم استاندارد BS7799 که در سال ۲۰۰۲ منتشر شد، به بیان جزییات استقرار فرآیند مدیریتی مورد نیاز جهت راه‌اندازی، بهره‌برداری، نگهداری و بهبود یک سیستم مدیریت امنیت اطلاعات[۵] پرداخته است. این بخش از استاندارد در واقع راهنمایی برای انتخاب کنترلهای مورد نیاز سازمانها بر اساس اهداف و نیازهای امنیتی آنان به‌شمار می‌رود. هدف نهایی استاندارد BS7799 فراهم نمودن یک طرح توسعه سازمانی است که در آن سیستم مدیریت امنیت اطلاعات قابل اجرا باشد. این استاندارد با رویکرد غلبه بر تمام محدودیتهای پیش‌رو، اعم از مشکلات بخشی، اندازه سازمان و ساختار موجود طراحی شده‌است.
به‌همین خاطر یک چرخه ایمن‌سازی را به‌منظور پیاده‌سازی و انتخاب کنترلهای مورد نیاز سازمان معرفی می‌کند. این چرخه همان‌طور که در شکل ۱ مشهود است، پویا می باشد و دارای چهار مرحله است : طراحی یک چارچوب امنیتی در سازمان و تصمیم‌گیری در مورد مسایل امنیتی، اجرای تصمیم‌گیری‌های مرحله اول، نظارت بر عملکرد سیستم مدیریت امنیت اطلاعات و اصلاح و بازنگری.



شکل ۱- چرخه ایمن‌سازی سازمان
منبع: (Hone and Eloff , 2003)

مرحله اول : در مرحله اول استقرار سیستم مدیریت امنیت اطلاعات بایستی تمام تحلیلها وتصمیم‌گیری‌ها، انجام شده و آماده پیاده‌سازی شود. به‌همین منظور شش گام مطابق شکل ۲ برای گذار از مرحله اول باید صورت گیرد:

تدوین خط مشی امنیتی سازمان : در این بخش سازمان بایستی برای خود مشخص کند که هدف و منظور وی از برقراری امنیت چیست؟ خروجی این گام سند خط‌مشی امنیت سازمان است که در آن مدیریت سازمان علاوه بر بیان منظور و هدف خود از برقراری امنیت، بایستی پشتیبانی و حمایت خود را از اجرای آن به‌صورت واضح بیان کند.



شکل ۲- گامهای لازم برای گذر از مرحله اول چرخه ایمن‌سازی
منبع : (خالقی،۱۳۸۳)

تعریف محدوده سیستم مدیریت امنیت اطلاعات و تبیین مرزهای آن در سازمان: در این بخش باید ویژگیها، مشخصه‌های اصلی و محدوده جغرافیایی سازمان مشخص شوند و پس از آن منابع اصلی و باارزش سازمان مانند تجهیزات و فناوریها به‌صورت کلی تعیین شوند.

ارزیابی مخاطرات : در این بخش عملیات ارزیابی مخاطرات صورت می‌گیرد. برای این کار ابتدا

باید دارایی‌های سازمان مشخص شوند، ارزش‌گذاری شوند و بر اساس نتایج آن گروه‌بندی شوند. پس از آن باید تهدیدها و شکافهایی که متوجه هر گروه است شناسایی شوند و تاثیر هر کدام از تهدیدها بر دارایی‌ها مشخص شود و درجه هر مخاطره نیز بایستی مشخص شود.

مدیریت مخاطرات سازمان: در این بخش مدیریت مخاطره با تعیین درجه اطمینان مورد نیاز سازمان جهت عدم وقوع هر یک از مخاطرات صورت می‌گیرد.

انتخاب و پیاده‌سازی کنترلها: بر اساس ارزیابی صورت گرفته در تشخیص و مدیریت مخاطره، هر سازمان بایستی با انجام یک فرآیند تحلیل و مدیریت مخاطره به‌طور مستند و مستدل نشان دهد که :

- چرا هر کنترل انتخاب شده‌است؟
- چرا بعضی از کنترلها انتخاب نشده‌اند؟
- چرا کنترل خاصی که در بخش اول استاندارد نیست و سازمان بنابر شرایط ویژه خود لازم شناخته است، انتخاب شده و چه کنترل‌هایی را شامل می‌شود؟

تدوین بیانیه کاربرد : آخرین بخش از مرحله اول ایجاد سیستم مدیریت امنیت اطلاعات، صدور سندی است که اقدامات مورد نیاز برای پیاده‌سازی سیاست امنیت اطلاعات را تعریف کند. در این مستند باید کلیه هزینه‌های اجرایی، زمان‌بندی و هم‌چنین سرمایه‌گذاری‌های لازم نیز شرح داده‌شوند.

مرحله دوم : پیاده‌سازی طرح در دو قسمت صورت می‌گیرد، اول پیاده‌سازی و اجرای سیاست‌های امنیتی، کنترلها و پردازشها است و دوم آموزش و آگاهی‌رسانی به کلیه کارکنان سازمان.

مرحله سوم : این مرحله را می‌توان مرحله ارزیابی نامید. همه محافظهایی که انتخاب شده‌اند برای کارکرد صحیح نیاز به نگهداری مداوم دارند. به‌جرات می‌توان گفت این مرحله از پیاده‌سازی امنیت، مهمترین قسمت آن است که اغلب به فراموشی سپرده می‌شود. علاوه بر نگهداری، هر سیستم نیاز به بازرسی و بررسی رویدادها و حوادث دارند که این مهم به‌خوبی در چرخه حیات سیستم مدیریت امنیت اطلاعات قابل مشاهده است. در مرحله ارزیابی، موفقیت و احیاناً شکست‌هایی که در اجرای سیاستهای تدوین شده پیش آمده، بررسی می شود. مرور نتایج حاصل از این مرحله ما را در داشتن دیدی بهتر و اصلاح خطاها هدایت می کند.

مرحله چهارم : هدف اصلی از این مرحله بهبود و ارتقای سیستم مدیریت امنیت اطلاعات است. این مرحله با ترمیم و تصحیح خطاهای مشاهده شده بر مبنای نتایج به‌دست آمده از مراحل قبل صورت می‌گیرد.

پس از پایان مرحله چهارم، چرخه ایمن‌سازی دوباره به مرحله اول یعنی طراحی بر می‌گردد. در زمان بازگشت به‌طور قطع تغییراتی در دارایی‌ها و یا ساختار سازمان صورت گرفته است. این تغییرات باید در سند امنیت اطلاعات ثبت شود و بر اساس آن کنترلهای لازم و هم‌چنین

موارد ترمیمی و اصلاحی به‌منظور بهبود و ارتقای سیستم مدیریت امنیت اطلاعات، در آن سند گنجانده شود.

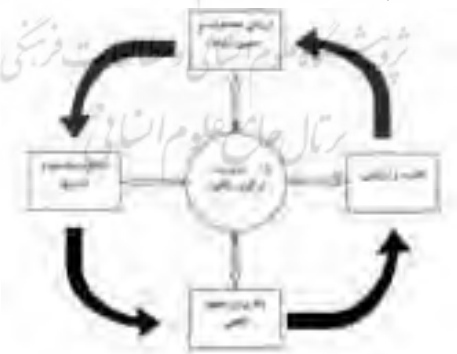
روش سازمان حسابرسی فدرال امریکا

درسال ۱۹۹۸سازمان حسابرسی فدرال[۶] گزارشهایی به مجلس سنای امریکا ارایه داد که شامل نکاتی درمورد ضعفهای امنیتی سیستمهای اطلاعاتی بود.درآن گزارش چنین آمده‌بود « هرچه تکیه دولت برفناوری اطلاعات بیشتر شود، مخاطراتی که ممکن است امنیت ملی را تهدید کند و یا باعث کاهش ارایه خدمات به مردم شود، افزایش می‌یابد».

با این اعتقاد، سازمان حسابرسی فدرال پژوهشها و بررسی‌های بسیاری در سازمانهای دولتی ایالات متحده انجام داد. نتایج این بررسی ها چنین گزارش شد: «ضعف اصلی در بروز مخاطرات امنیتی سیستم‌های اطلاعاتی، نبود سازوکاری جهت مدیریت امنیت تشخیص داده‌شد». در نهایت بر مبنای نتایج به‌دست آمده از این پژوهشها، سازمان حسابرسی فدرال الگوی «اصول مدیریت خطر[۷] » را برای کلیه سازمانهای دولتی کشور امریکا ارایه کرد که مورد حمایت مجلس سنا نیز قرار گرفت.

اصول مدیریت خطر یا چرخه مدیریت خطر با هدف برنامه‌ریزی موثر برای حفاظت اطلاعات طراحی شده است و چارچوب خوبی را برای برقراری امنیت در سازمان‌هایی که بر فناوری اطلاعات تکیه دارند، ارایه می‌کند. در شکل ۳ چرخه مدیریت خطر نمایش داده شده است.

این چرخه به‌طور مداوم خطرات فناوری، تجارت، سیاست‌های طراحی شده، کنترل‌ها و عملیاتی را که در فرآیندهای موازی صورت می‌گیرد به‌وسیله کنترل‌هایی که در سیستم تعبیه شده بازنگری می‌کند. عناصر این چرخه عبارتند از :



شکل ۳- چرخه مدیریت خطر منبع : (GAO,1998)

ایجاد مدیریت مرکزی با نفوذ

• تشکیل یک گروه مرکزی برای انجام فعالیتهای کلیدی: این گروه به منظور برآورده ساختن نیازهای امنیتی، طبق برنامه‌های مناسب و مداوم به سازماندهی امور مربوط به سیستمهای اطلاعاتی می‌پردازد.

• ارتباط گروه مرکزی با مدیران ارشد و مدیران فناوری اطلاعات: اصولاً این گروه واسط بین مدیران ارشد و متولیان شبکه و کاربران هستند.

• تعیین بودجه و کارکنان: تعیین بودجه مورد نیاز برای به‌روزرسانی تجهیزات سخت‌افزاری و نرم‌افزاری، پرداخت حقوق کارکنان بخش فناوری اطلاعات و هزینه‌های آموزشی به‌عهده این گروه است. علاوه بر این، گروه امنیت با توجه به شرایط محیط در مواقعی که سازمان دچار ضعف امنیت اطلاعاتی شود، اقدام به جذب نیروهای متخصص می کند.

• بالا بردن مهارتهای فنی گروه امنیت: تعلیم و تربیت کارکنان گروه مدیریت امنیت اطلاعات با سایر کارکنان تفاوت دارد، زیرا این حوزه به‌طوردایم در حال تغییر و دگرگونی است. کارکنان این گروه باید به‌طورمستمر با سازمان در کنفرانسهای فنی و تکنیکی و دوره‌های تخصصی با موضوعات امنیت نرم‌افزار و شبکه و مطالعه بولتن‌ها وسایر مستندات منتشر شده، اطلاعات خود را به‌روز نگه دارند.

ارزیابی خطر و تعیین نیازها

• تشخیص منابع اطلاعاتی : سازمان باید اطلاعات و سیستمهای اطلاعاتی خود را به‌عنوان سرمایه اصلی خود دانسته و همواره در جهت حفظ و نگهداری آن کوشش کند.

• فرایند ارزیابی مخاطرات : سازمان باید به‌صورت آزمایشی به کاوشهای مختلف جهت ارزیابی خطر در سیستم‌های خود پرداخته و نقاط ضعف آنها را منصفانه ارایه کند و پس ازآن به رفع مشکلات بپردازد.

• تحولات امنیتی باید به سرعت به مدیران ارشد سازمان گزارش داده شود.

• کنترل خطر در مراحل اولیه : مدیریت مرکزی همواره باید هوشیار باشد و با نظارت بر روی سیستم‌های اطلاعاتی آدرس کسانی که ناآشنا هستند یا بدون مجوز وارد سیستم می‌شوند به‌دست آورد، و خیلی سریع واکنش نشان دهد.

بکارگیری خط‌مشی‌های صحیح و کنترلهای لازم

• ایجاد ارتباط بین سیاستهای کاری و ریسک‌های تجاری: تاکید سازمانها بر اهمیت به‌روزرسانی

سیاستها با توجه به محیط اطراف و تغییرات آن ضروری است.

• تعیین سیاستها و راهبردها : سیاستها نمایی از الزامات اساسی هستند که به‌وسیله مدیر ارشد مطرح می‌شود و اجرای آن ضروری است. رهنمودها نیز شامل جزییات اجرایی سیاستها می‌باشد.

• پشتیبانی از سیاستها توسط گروه امنیت : گروه مرکزی امنیت عهده‌دارگسترش و مکتوب کردن سیاستها با مشارکت مدیران تجاری، حقوق‌دانان و کارشناسان فناوری اطلاعات است.

بالا بردن سطح آگاهی

• آموزش مداوم تمامی استفاده‌کنندگان در زمینه فناوریهای اطلاعات : برای اجرای سیاستهای امنیت اطلاعات، آگاهی دادن به کاربران، از کارهای بسیار حیاتی و لازم است. کاربران و دیگر کسانی که به منابع اطلاعاتی دسترسی دارند به‌واسطه عدم دقت و یا عدم آگاهی توانایی پیش‌بینی خطرات را ندارند.

• بهره‌گیری از فنون جلب توجه : آموزش و ترویج تکنیک‌های حفاظت و ایجاد حساسیت در کاربران به‌منظور جلوگیری از لو رفتن اطلاعات بر اساس سیاستهای تدوین شده، بسیار مفید خواهد بود.

نظارت و ارزیابی

• نظارت بر روی فاکتورهایی که بر ریسکها اثر می‌گذارد و اثربخشی امنیتی را مشخص می‌کند، مانند تعیین شروط کنترل مکانها و عملیات کاهش ریسک و همچنین ارزیابی کارآیی برنامه‌های امنیتی، سیاستهای تدوین شده و ارتقای سطح آگاهی کاربران.

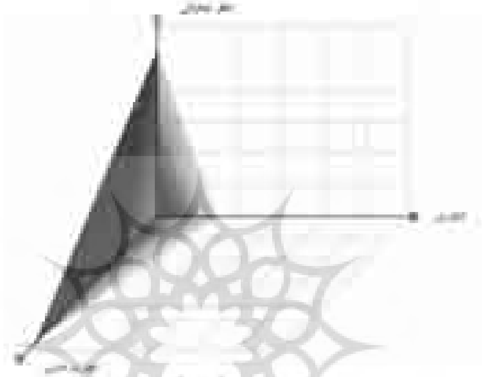
• استفاده از نتایج : گرچه بازنگری به تنهایی قادر است سیاست‌های امنیت اطلاعات را تقویت کند، اما کافی نیست و می‌بایست از نتایج حاصل از آن برای بهبود امنیت استفاده کرد.

• به‌روز بودن تکنیکها وابزارهای نظارتی : استفاده از شیوه‌های جدید کدنویسی در تهیه نرم‌افزارها و همچنین بکارگیری ابزارهای نظارتی جدید که بر آسیب‌پذیری‌های شبکه نظارت می‌کنند، کمک موثری در افزایش ایمنی خواهد داشت.

روش اکتاو

روش اکتاو در سال ۱۹۹۹ توسط انستیتو مهندسی نرم افزار دانشگاه کارنگی ملان[۸] ایالات متحده امریکا توسعه یافته و بر تحلیل مخاطرات دارایی‌های فناوری اطلاعات و راه حل‌های

عملی برای کاهش عوامل خطر به‌واسطه غلبه بر معایب امنیتی کشف شده تمرکز دارد. اکتاو برای سازمانهایی طراحی شده‌است که می‌خواهند نیازهای مربوط به امنیت اطلاعات‌شان را شناسایی کنند. اکتاو« خود هدایت شده» است، به این معنی که کارکنان سازمان برای استقرار راهبرد امنیت، مسئولیت به‌عهده می‌گیرند. این روش، از دانش افرادی که با تکنیکها و فرآیندهای مرتبط با سازمان آشنایی کامل دارند به‌عنوان اهرم استفاده می کند تا وضعیت جاری مربوط به رویه امنیتی داخل سازمان را کنترل کند.



شکل ۴ – ابعاد سه گانه اکتاو (Alberts & Dorofee،2001)

بر خلاف سایر روشها که بر ابعاد فناورانه متمرکز می‌باشد، روش اکتاو بر موضوعهای راهبردی متمرکز است. اکتاو، خطرات سازمانی را هدف قرار می دهد و بر موضوعهای راهبردی مرتبط با تجربه کارکنان تمرکز دارد. اکتاو یک روش ارزیابی انعطاف‌پذیر است که می‌تواند برای اغلب سازمانها مناسب باشد. برای اجرای روش اکتاو، گروه کوچکی از افراد از واحدهای عملیاتی (یا تجاری) و بخش فناوری انتخاب می‌شوند، این افراد سازمان را قادر می‌سازند تا دیدگاه مربوط به فنون امنیتی جاری را تصحیح کنند. با به‌کار بردن روش اکتاو، سازمان تصمیمات مربوط به حفاظت اطلاعات را بر اساس خطراتی که در برابر محرمانه

[illegible]

در تصمیم‌گیری به حساب آورده می‌شوند تا سازمان را قادر سازد که راهبرد حفاظتی مناسبی

بر اساس فنون رایج انتخاب کند. جدول ۱ تفاوتهای اصلی بین اکتاو و دیگر ارزیابی‌ها را به‌طور خلاصه مطرح می‌کند.

ویژگی‌های روش اکتاو	ویژگی‌های سایر روش‌های ارزیابی
ارزیابی سازمانی	ارزیابی سیستمی
تمرکز بر امنیت	تمرکز بر فناوری
موضوعات راهبردی(استراتژیک)	موضوعات تکنیکی
خود رهبری	هدایت شده از سوی کارشناس

جدول ۱ - تفاوتهای اصلی بین اکتاو و روش‌های دیگر(Alberts & Dorofee،2001)

ویژگیهای کلیدی روش اکتاو

اکتاو خود هدایت شده است و نیاز به سازمانی دارد تا فرآیند ارزیابی را اداره کند و تصمیمات مربوط به حفاظت اطلاعات را اتخاذ کند. یک گروه متشکل از رشته‌های مختلف علمی به‌نام گروه تحلیل، ارزیابی را رهبری می کند. این گروه شامل افرادی از واحدهای تجاری و بخش فناوری اطلاعات است. گروه‌های تحلیل اقدامات زیر را انجام می‌دهند:

• دارایی‌های مرتبط با فناوری اطلاعات (مانند اطلاعات وسیستم) را که برای سازمان مهم می‌باشند شناسایی می کنند.

• فعالیت‌های مربوط به تحلیل خطر را بر روی آن دارایی هایی متمرکز می‌کنند که برای سازمان از همه حساس‌تر تشخیص داده‌می‌شوند.

• روابط بین داراییهای حساس، تهدیدهای پیش‌روی آن داراییها و آسیب‌پذیریهایی که می‌توانند داراییها را در معرض تهدید قرار دهند (اعم از آسیب‌پذیری‌های سازمانی و فناورانه) را در نظرمی‌گیرند.

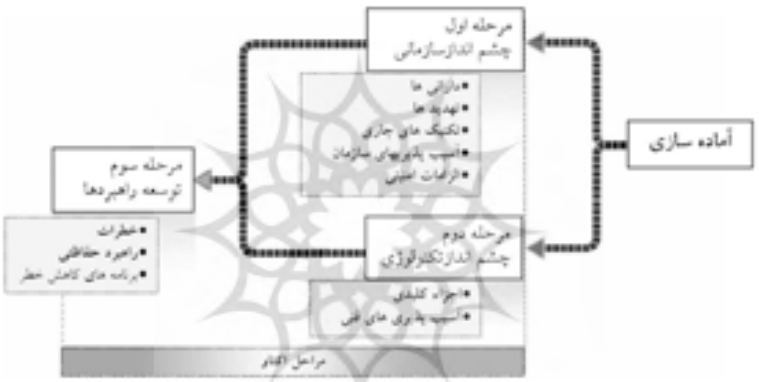
• خطرات را در بافت عملیاتی ارزیابی می‌کنند، به این ترتیب که بررسی می کنند دارایی های سازمان چگونه باعث گسترش فعالیتهای سازمان می شوند و چگونه ممکن است در برابر تهدیدات امنیتی قرار گیرند و با خطرمواجه شوند.

• برای کاهش خطرات مترتب بر دارایی‌های حساس سازمان، راهبرد حفاظت بر اساس تکنیکهای مناسب جهت بهبود عملیات سازمانی و هم‌چنین برنامه‌های کاهش خطر را معرفی کنند.

جنبه‌های سازمانی، فناورانه و تحلیلی ارزیابی خطر مربوط به امنیت اطلاعات به‌وسیله روش

سه مرحله‌ای تکمیل می شود. اکتاو پیرامون این سه جنبه اساسی (توضیح داده شده در شکل۵) سازمان داده می‌شود، و کارکنان سازمان را قادر می‌سازد تصویر جامعی از نیازهای مربوط به امنیت اطلاعات سازمان را فراهم کنند.

• **مرحله ۱ : ساختن نمودار سطح خطرات بر اساس دارایی‌ها** : این یک ارزیابی سازمانی می‌باشد. گروه تحلیل تعیین می‌کند که چه چیزی برای سازمان مهم است (داراییهای مرتبط به فناوری اطلاعات) و چه کاری برای محافظت از آن داراییها به انجام می‌رسد. سپس گروه تحلیل آن دارایی‌هایی را که از همه برای سازمان مهمتر است (دارایی‌های حساس) انتخاب می کند و الزامات امنیتی برای هر دارایی حساس را توصیف می‌کند. سر انجام تهدیدات در برابر هر دارایی حساس را با ایجاد نمودار تهدید برای آن دارایی تعریف می‌کند.



شکل ۵ – مراحل اکتاو (Alberts & Dorofee،2001)

• **مرحله ۲** : شناسایی زیرساختهای آسیب‌پذیر: این قسمت ارزیابی اطلاعات زیربنایی است. کلید اجرایی جزییات این قسمت از زیربنای فناوری اطلاعات با اطلاعات گردآوری شده در مرحله اول تشخیص داده می‌شود و سپس برای نقاط ضعفی که می‌توانند اعمال غیر معتبر را رهبری و هدایت کنند (آسیب‌پذیری‌های فناورانه) آزمایش می‌شود.

• **مرحله ۳** : گسترش استراتژی امنیتی و نقشه‌های مربوط: در این مرحله میزان خطرپذیری سیستمهای اطلاعاتی بررسی می‌شود. اطلاعات تولید شده در مرحله یک و دو بررسی می‌شوند تا احتمال ضرر و زیان تشخیص داده شود و احتمال خطر در ماموریت سازمان ارزیابی شود.

سرانجام یک استراتژی محافظتی برای سازمان تدوین می‌شود که در آن بسته به اهمیت سیستمها و تجهیزات فناوری اطلاعات، روشهایی برای کاهش خطر پذیری آنها ارائه می‌شود.

اکتاو بخشی از زنجیره ایمن‌سازی

ارزیابی مخاطرات مربوط به امنیت اطلاعات، بخشی از فعالیتهای سازمان برای کنترل خطرات امنیت اطلاعات است. اکتاو یک فعالیت ارزیابی است، نه فرآیندی مستمر. بنابراین آغاز و پایانی تعریف شده دارد. شکل ۶ ارتباط این فعالیت‌ها و جایی که اکتاو به‌منظور ارزیابی مورد استفاده قرار می‌گیرد را نمایش می‌دهد.

بخشی از فعالیتهای نشان داده شده در شکل ۶ که شامل برنامه‌ریزی، اجرا، نظارت و کنترل می‌باشد در واقع همان چرخه مدیریت خطر در شیوه سازمان حسابرسی فدرال و چرخه ایمن‌سازی در استاندارد BSV۷۹۹ است.

شکل ۶ - **فعالیتهای اکتاو و مدیریت خطر** (Alberts & Dorofee،2001)

فرآیند پیشنهادی حاصل از پژوهش جهت اجرای سیستم مدیریت امنیت اطلاعات

در این فرآیند روش اجرایی ارایه می شود تا با استفاده از آن مخاطرات استفاده از فناوری اطلاعات در سازمانها به حداقل برسد. بیشاپ[۹] (2003) در مقاله‌ای تحت عنوان امنیت کامپیوتر

چیست؟ می‌نویسد برای برقراری موفقیت‌آمیز امنیت در هر سیستمی باید سه پارامتر زیر مشخص شوند:

• هدف از امنیت : در این مولفه باید به این سوال پاسخ داد که سازمان از امنیت چه می‌خواهد و برای چه به‌دنبال امنیت است.

• سیاست امنیتی : در این مولفه، روش رسیدن به هدف و گام‌هایی که باید برای رسیدن به آن برداشت، مستقل از پیاده‌سازی مشخص می‌شود.

• سازوکارهای امنیتی : در این مولفه سازوکارهای فنی و غیرفنی برای پیاده‌سازی سیاست‌ها مشخص می‌شود(Bishop. M، 2003).

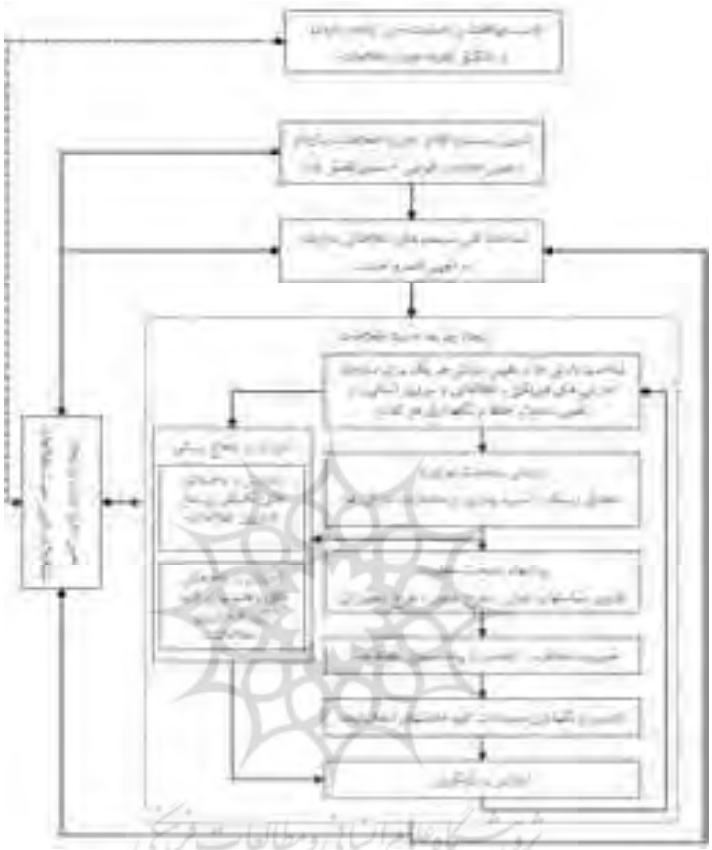
در مقدمه مقاله دلایل ایجاد سیستم امنیتی چنین بیان شد: حفظ اطلاعاتی که در قالب طرحها، نقشه‌ها، سیاستها، بخشنامه‌ها، مکاتبات تجاری و اداری، مستندات پروژه‌های تحقیقاتی و سایر اطلاعاتی که ما برای ذخیره‌سازی و پردازش در اختیار فناوری اطلاعات قرار می‌دهیم.

درشکل۷ روش اجرایی آورده شده است. هدف ما از ارایه این روش، شناسایی مولفه‌ها و شاخصهای اساسی برای ایمن‌سازی فضای تبادل اطلاعات در سازمان است. این روش با بهره‌گیری از مطالعات جامعی که بر روی استانداردها و روشهای ایمن‌سازی انجام گرفته، طراحی شده‌است. همچنین در طراحی روش سعی شده است بخش‌هایی که از نظر محتوا با ساختار سازمانها سازگاری بیش‌تری دارند انتخاب شوند. روش پیشنهادی استقرار سیستم مدیریت امنیت اطلاعات شامل یازده مرحله است که در ادامه به بررسی هر یک از این مراحل می‌پردازیم:

کسب موافقت و حمایت مدیر ارشد سازمان و تشکیل کمیته امنیت اطلاعات

همانگونه که عنوان شد حمایت مدیر ارشد سازمان از مبانی اساسی پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سازمان است؛ این حمایت بر کل سازمان اثر می گذارد و همکاری تمامی کاربران و مدیران را جلب می کند. به‌عبارت دیگر امنیت باید به‌شکل نظام واحد در آید تا به‌نتیجه برسد و به‌طور قطع بدون حمایت مدیر ارشد سازمان، پیاده‌سازی موفق امکان‌پذیر نخواهد بود.

پس از اخذ حمایت همه جانبه مدیر ارشد سازمان، نوبت تشکیل کمیته امنیت اطلاعات است. این کمیته دو وظیفه عمده برعهده دارد اول تعیین مدیر امنیت اطلاعات و دوم تشکیل منظم جلسه به‌منظور نظارت مستمر بر نحوه اداره سیستم مدیریت اطلاعات(خالقی. ،۱۳۸۳).



شکل ۷ – مدل پیشنهادی استقرار سیستم مدیریت امنیت اطلاعات

اعضای کمیته امنیت را می توان از مدیر ارشد سازمان، معاون طرح و برنامه، مدیر فناوری اطلاعات، مدیر حراست و مدیر امنیت اطلاعات سازمان تشکیل داد.

تعیین مدیر امنیت و ایجاد تشکیلات تامین امنیت اطلاعات

پس از تشکیل جلسه کمیته امنیت اطلاعات، بایستی مدیر امنیت تعیین شود. مدیر امنیت بایستی با انتخاب و جذب خبرگان فن امنیت اطلاعات، تشکیلات تامین امنیت اطلاعات را راه‌اندازی کند(خالقی. ،۱۳۸۳).

تدوین سیاست کلان امنیت اطلاعات سازمان

انستیتو بین‌المللی استاندارد و فناوری[10] (1995) سیاست امنیتی را چنین تعریف می‌کند: سیاست امنیتی، سندی است که شرایط مورد انتظار امنیتی و مقررات کلان مربوط به آن‌را در سطح سازمان بیان می‌کند. این سند باید به‌طور صریح و دقیق مشخص کند چه سطحی از امنیت برای سازمان مورد انتظار است. سادوسکای [11] در کتاب راهنمای امنیت اطلاعات معتقد است سیاست امنیت اطلاعات در سازمان باید سه نقش عمده ایفا کند. اول مشخص کند از چه چیزی باید حفاظت شود و چرا، دوم این که چه کسی از آن حفاظت کند و سوم این‌که زمینه‌ای برای تفسیر و حل درگیریهایی که ممکن است در آینده پیش‌آید ارایه کند(Sadowsky et al ،2003).

در ادامه سادوسکای در همان کتاب می‌نویسد: سیاست امنیتی سازمان نباید شامل تهدیدها، تجهیزات و افراد (با نام هایشان) باشد. همچنین سیاست امنیتی باید کلی باشد و در طول زمان به‌ندرت دچار تغییر شود.

هدف از تدوین سیاست امنیتی سازمان آن است که کاربران، مدیران و بخصوص متولیان امر فناوری اطلاعات از وظایف خود و کارهایی که برای ایمن سازی داراییهای اطلاعاتی و تجهیزات فنی سازمان لازم است، اطلاع یابند و از بروز سوء تفاهم و ابهام جلوگیری کنند. سیاست امنیت برای ایجاد وحدت در کارکرد تمام عوامل ایمن‌سازی لازم است (Hone & Eloff،2003).

سیاست امنیت اطلاعات باید شامل مرجعی باشد تا به‌کمک آن بتوان بر حسن اجرای کار نظارت کرد و در صورت تخطی از آن، عواقبی را برای متخلفان در نظر گرفت. سیاست امنیتی باید توسط تشکیلات امنیت سازمان و در صورت نیاز اخذ کمک از مشاوران خارج سازمان تدوین و توسط یک متخصص رسمی مدیریت امنیت اطلاعات مورد بازبینی قرار گیرد. پس از آن به تصویب مدیر ارشد سازمان رسانده شود و در آخر نیز به رویت کلیه کاربران و مدیران آنها برسد. **ولد**[12] (2004) در تحقیقی تحت عنوان «عوامل کلیدی در تدوین سیاست امنیتی موثر» که در کشور نروژ انجام شد به این نتیجه رسیده که اگر کاربران از ارزش سیاست اطلاعاتی مطلع نباشند، آن‌را به عنوان یک کار احمقانه تلقی می‌کنند و هرگز از آن پیروی نخواهند کرد.

هون و الوف[13] (2003) در مقاله «چگونه سیاست امنیت اطلاعاتی موثر ایجاد کنیم» نوشته‌اند: اغلب کاربران از وجود سیاست اطلاعاتی یا مطلع نیستند و یا آن را کاملا درک نمی‌کنند. آنها معتقدند سیاست‌ها خیلی طولانی یا خیلی فنی هستند و کاربران رابطه‌ای بین وظایف روزانه خود و سیاست امنیت اطلاعات نمی‌بینند و اغلب آن‌را مایه رنجش می‌دانند؛ در نتیجه از آن تبعیت نمی‌کنند.

هدف از نقل این بیانات این است که اهمیت سیاست امنیت اطلاعات در استقرار سیستم مدیریت

اطلاعات را درک کرده و بدانیم که چگونه آنرا تهیه کنیم تا علاوه بر دستیابی به اهداف امنیتی، بیشترین سود را از مشارکت کلیه کاربران ببریم.

شناخت کلی سیستم‌های اطلاعاتی سازمان و تعیین قلمرو امنیت

در گام بعدی پیاده‌سازی سیستم مدیریت امنیت اطلاعات باید حیطه امنیت تعیین شود. حیطه امنیت می‌تواند کل سازمان و یا بخشهایی از سازمان باشد که امنیت آن از اولویت بالاتری برخوردار است.

آموزش و اطلاع رسانی

در مدل پیشنهادی با توجه به اهمیت نیروی انسانی، بعد از تدوین و تصویب سیاست کلی سازمان باید کلیه کاربران از مفاد آن مطلع شوند و در صورت نیاز با برقراری جلسه های توجیهی، سطح آگاهی کاربران ارتقا یابد. بسیاری از پژوهشها نشان می‌دهند بیش از ۸۰ درصد مشکلات امنیتی در سازمانها ناشی از خطاهای سهوی و عمدی کارکنان بوده است (Sadowsky et al ،2003). خطا های عمدی در جای خود بحث خواهد شد، اما خطاهای سهوی اکثرا به دلیل عدم آگاهی به‌وجود می‌آید. از این رو کاربران همواره باید از مخاطراتی که داراییها را تهدید می‌کنند مطلع باشند. ضمن این‌که آموزش نحوه مقابله با آن‌ها باعث مسئولیت‌پذیری کاربران می شود و به رفتار معقول آنها در مقابله با خطرات کمک می‌کند. در مدل ارایه شده آموزش شامل دو بخش «آموزش و راهنمایی‌های تکنیکی کارکنان فناوری اطلاعات» و «آموزش و راهنمایی‌های منظم برای کلیه کاربران فناوری اطلاعات» است.

آموزش مداوم تکنیکی کارکنان فناوری اطلاعات به‌دلیل تحولات بسیار سریع فناوری و هم‌چنین وابستگی شبکه، نرم افزار و سخت افزار به این گروه از اهمیت بالایی برخوردار است. این گروه با کسب آخرین تحولات امنیتی در جهان می‌توانند به ایمن‌سازی حوزه فعالیت خود بپردازند و وظیفه آموزش سایر کاربران را برقراری کلاس، سمینار آموزشی، انتشار بولتن و یا احداث وب سایت جذاب که توانایی جذب مخاطبان را داشته باشد، برعهده بگیرند.

شناخت داراییها و تعیین ارزش هر یک برای سازمان

هدف از این مرحله شناخت جنبه‌های گوناگون دارایی‌ها وتعیین ارزش هر یک می‌باشد. در توضیحات مربوط به استاندارد BSv۷۹۹ در کنترل طبقه‌بندی و کنترل داراییها، کنترل امنیت نیروی انسانی، کنترل امنیت فیزیکی، مرحله ارزیابی خطر و تعیین نیازها در روش سازمان حسابرسی فدرال به‌تفصیل راجع به این مرحله توضیح داده شده است.

ارزیابی وضعیت موجود (تحلیل خطر)

بیسون (2004) که یکی از تحلیل‌گران ارشد شرکت کالیو[۱۴] می‌باشد در مقاله BS7799 و ISO17799 شیوه‌ای برتر برای امنیت اطلاعات پیشنهاد می‌کند گام سوم در استقرار سیستم مدیریت امنیت اطلاعات به دو مرحله ارزیابی وضعیت موجود و پیشنهاد وضعیت مطلوب تقسیم‌بندی شود. دلیل ما برای تفکیک، تقلید کورکورانه نیست، بلکه تجربه موفق ده ساله کالیو این اطمینان را به ما می‌دهد که حداقل برای یک بار دو مرحله فوق را در چرخه ایمن‌سازی سازمانها به‌کار گیریم. پس از آن، اگر این روش موفق بود در دورهای بعدی چرخه ایمن‌سازی آن را تثبیت کنیم و در صورت عدم موفقیت می‌توانیم ارزیابی مخاطرات را که در استاندارد ذکر شده، لحاظ کنیم. هدف از این مرحله شناسایی آسیب‌پذیریهای امنیتی دارایی‌های شناسایی شده در مرحله قبل است. در این مرحله با استفاده از روش اکتاو، اطلاعات مهم و با ارزش سازمان و تهدیدات علیه آنها و امنیت مورد نیاز این داراییها تشخیص داده می‌شود.

تحلیل درست خطر، نقش عمده‌ای را در پیش‌برد صحیح کارها بر عهده دارد. تحلیل خطر فرآیندی است که بر طبق آن دارایی‌های اطلاعاتی مهم سازمان، چگونگی کاربرد و عملکرد آنها مشخص می‌شود. در این مرحله به‌طور دقیق مشخص می‌شود که «چه» چیزی را می‌خواهیم محافظت کنیم، این حفاظت در برابر «چه کسی» صورت می‌گیرد و در نهایت «چگونه» این حفاظت می‌خواهد صورت پذیرد. جهت انجام یک تحلیل ریسک موفق ابتدا باید عملکرد سازمان، رویه‌های تجاری گوناگون ومنابع اطلاعاتی مهم، شناخته شوند. باید تعیین شود که چه وسایل و رویه‌هایی می‌توانند یک مشکل امنیتی احتمالی را به‌وجود آورند. جهت اطمینان و دقت بیشتر، بهتر است که تمامی آنها لیست شوند. برای این منظور بایستی مراحل زیر انجام گیرد:

- آنچه را که باید محافظت شود به طور دقیق مشخص می شود.
- باید مشخص شود در برابر چه کسی و یا چه چیزی حفاظت باید انجام شود.
- باید به‌طور دقیق مشخص کرد که برای هر یک از داراییهای اطلاعاتی چه خطراتی وجود دارد.
- باید فرآیند ارزیابی به‌صورت مستمر به‌هنگام شود تا این‌که نقاط ضعف امنیتی برطرف شوند.
- لیستی از سخت‌افزارهای گوناگون نظیر ایستگاه‌های کاری، کامپیوترهای شخصی، کامپیوترهای کیفی، رسانه‌های قابل جابجایی (مانند CD، فلاپی، نوار) و خطوط ارتباطی تهیه شود.
- در بعد نرم‌افزاری میزان خطر و مشکلات امنیتی بالقوه ناشی از نرم افزارهای رایج،

به‌هنگام‌سازی به نسخه های بالاتر و... مشخص شود. هم‌چنین مشکلات بالقوه ناشی از نصب نرم‌افزارهای گوناگون بخصوص نرم‌افزارهای اشتراک فایل، نرم‌افزارهای بازی و سرگرمی توسط کاربران بدون مجوز کنترل شوند.

• در مورد کارکنان نیز نسبت به افرادی که دسترسی به اطلاعات محرمانه و داده‌های حساس دارند و یا می‌توانند پایگاه‌های داده فعلی را تغییر دهند حساسیت بالایی وجود داشته باشد (کریم بیگی،۱۳۸۴).

پیشنهاد وضعیت مطلوب (تدوین سیاست‌های جزیی، طرح تجهیزاتی)

پس از آن‌که آسیب پذیریها مشخص شد، نوبت ارائه طرحی است که شرایط مطلوب را پیشنهاد می‌کند. در این طرح سیاستهای امنیتی سطح دو [۱۵] که به بیان جزییات می‌پردازد ارایه می‌شود و پس از آن چنان‌که جهت برقراری امنیت تجهیزاتی نیاز باشد، مشخص می شود.

مدیریت مخاطره (انتخاب و پیاده سازی حفاظ‌ها)

در این مرحله لازم است بر اساس طرح تدوین شده در مرحله قبل، عملیات پیاده‌سازی انجام گیرد. استفاده از قسمت چهارم و پنجم گزارش فنی ISO/IEC TR۱۳۳۳۵ می تواند کمک به‌سزایی درجهت موفقیت این مرحله نماید.

تدوین و نگهداری مستندات کلیه فعالیت‌های انجام شده

به‌دلیل حجیم بودن فعالیت‌های انجام شده، از مطالعه اولیه تا پیاده‌سازی، لازم است کلیه فعالیت‌های انجام شده مکتوب و به‌صورت مناسب نگهداری شود. این مستندات در مواقع مرورهای دوره‌ای، جهت عدم تکرار رویه‌های ناموفق و هم‌چنین دریافت گواهی‌نامه سیستم مدیریت امنیت اطلاعات بسیار مفید واقع خواهند شد.

ارزیابی و بازنگری

در قسمت دوم استاندارد BS7799 ، یک مرحله به‌نام بازنگری و اصلاح وجود دارد. در روش سازمان حسابرسی فدرال نیز یک مرحله به‌نام نظارت و ارزیابی وجود دارد که هر دو آنها بر این نکته تاکید دارند که این مرحله موجب بهبود و ارتقای سیستم مدیریت امنیت اطلاعات می‌شود.

نتایج به‌دست آمده از پژوهش ولد(2004) در شناسایی عوامل موثر در پیاده‌سازی موفق امنیت اطلاعات این نکته را تایید می کند که «نظارت و بازنگری» از ارکان اساسی پیاده‌سازی سیستم مدیریت امنیت اطلاعات است. او هم‌چنین معتقد است که: «یک عمل را تا وقتی می توان اداره کرد که قابل اندازه‌گیری باشد». یکی از بخشهای اساسی سیستم مدیریت امنیت اطلاعات همین

مرحله است که معمولا به فراموشی سپرده می‌شود. این مرحله با ترمیم و تصحیح خطاهای مشاهده شده بر مبنای نتایج به‌دست آمده از مراحل قبل به اصلاح نقاط آسیب‌پذیر می‌پردازد.

مدل مفهومی پژوهش

امنیت اطلاعات حاصل نمی شود مگر آن که بتوانیم ابعاد مختلف آن شناسایی، و امنیت کامل تمامی آنها تامین شود. بدین منظور با مطالعه استانداردها و روشهای استقرار امنیت اطلاعات ابعاد گوناگون امنیت اطلاعات شناسائی شد. شکل ۸ مولفه ها و شاخص های اصلی امنیت اطلاعات که در واقع مدل مفهومی پژوهش می باشد رانشان می دهد.

شکل ۸ – مدل مفهومی پژوهش

امنیت فیزیکی

سیستمهای رایانه ای اهداف مناسبی برای تخریب هستند، دلایل تخریب می تواند شامل انتقام جویی، آشوب، اعتصاب، بیانیه های سیاسی و فکری و یا تنها سرگرمی برای نابخردان باشد(Sadowsky et al ،2003). اصولاً هر بخش یک سیستم رایانه ای، یا ساختمانی که آنرا در خود جای داده است ممکن است هدف تخریب قرار گیرد. به منظور کنترل این بعد از امنیت

اطلاعات شاخصهای زیر شناسایی شده اند:

- خطرات محیطی (صاعقه، سیل، زلزله، بمب‌گذاری، حملات تروریستی، قطع کابل ارتباط شبکه)
- سرقت (رایانه رومیزی، رایانه کیفی، قطعات رایانه ها)
- حفاظت از سخت افزار (دسترسی فیزیکی افراد غیر مجاز، حوادث مانند آتش‌سوزی و ترکیدگی لوله، دود، دما، پارازیت های الکتریکی، نصب تجهیزات استراق سمع)
- تعمیرات در خارج از سازمان

امنیت نیروی انسانی

ولد(2004) در قسمتی از پژوهش خود به یک واقعه تاریخی اشاره می کند: دراواخر سال ۱۲۰۰ میلادی **کوبلای خان** و ایل وتبار مغولی او سعی در عبور از دیوار چین داشتند، اما دیوار بسیار محکم، عمیق و طولانی بود. عاقبت به‌صورت آرام و ساکت، با تطمیع دروازه‌بان، ترتیبی اتخاذ کردند تا با پیروزی بر آن موانع، توانستند بخش بزرگی از کشور چین را فتح کنند. مفهوم این گفته این است که مهم نیست کنترلهای فنی چقدر قوی باشند، بلکه امنیت همیشه به افراد داخل سازمان بستگی دارد. هم‌چنین در کتاب «راهنمای امنیت اطلاعات» آمده که بسیاری ازپژوهشها نشان می‌دهند بیش از ۸۰ در صدمشکلات امنیتی پیش آمده در سازمانها ناشی از خطاهای سهوی و عمدی کارکنان بوده است(Sadowsky et al ،2003).

دو نقل بالا و کنترل «امنیت کارکنان» از بخش اول استاندارد BSVV۹۹ بر این نکته تاکید دارند که انسان خدشه‌پذیرترین عنصر در حلقه امنیت اطلاعات می‌باشد، از این‌رو توجه به آن ما را در رسیدن به حداکثر ایمنی کمک می‌کند. به دلیل اهمیت بسیار این مولفه به دو مولفه، آگاهی کاربران و امنیت نیروی انسانی(عوامل تحمیلی بر نیروی انسانی) تبدیل می شود تا این مولفه دقیقتر بررسی شود.شاخصهای موثر در امنیت نیروی انسانی که می‌توانند سبب بروز اختلال در فعالیتهای نیروی انسانی شوند، عبارتند از:

- کار زیاد
- نداشتن مهارت کافی ولازم
- تداخل مسئولیتها
- عدم اطلاع از میزان ارزش اطلاعات
- نداشتن انگیزه
- کوتاهی و بی‌مسئولیتی
- فراموش کاری

شاخصهای موثر که می‌توانند به دلیل عدم آشنایی کاربران سبب بروز اختلال درفعالیتهای نیروی انسانی شوند، عبارتند از:

- سیستم عامل
- سیستمهای کاربردی
- امنیت سیستم عامل
- بسته های نرم افزاری

امنیت تکنیکی

این قسمت روی مکانیزم هایی تمرکز دارد که اطلاعات را از انتشار نا خواسته، تحریف و یا تخریب حفاظت می کنند(Sadowsky et al.2003). این بعد از امنیت معمولاً محرمانگی نامیده می شود، که از دسترسی یا تغییر در داده ها، برنامه ها و یکپارچگی سیستم توسط کاربران غیر مجاز جلوگیری می کند و اطمینان می دهد اطلاعات و نرم افزار ها دست نخورده و صحیح باقی بمانند. برای کنترل این بعد از امنیت اطلاعات شاخصهای زیر شناسایی شده اند:

- افشای اطلاعات
- تغییر اطلاعات
- تخریب اطلاعات

سوالهای پژوهش

پژوهش حاضر ابتدا با مطالعات کتابخانه ای آغاز شد و پس از شناسایی عوامل اثر گذار در امنیت اطلاعات، مدل مفهومی طراحی و شاخصهای اثر گذار بر سیستم امنیت اطلاعات شناسایی شد که بر اساس این مطالعات چهار سوال اساسی و هفت سوال فرعی زیر مطرح شد. مرجع استخراج سوالها نیز لیست های ارزیابی استاندارد BS7799 ، روش سازمان حسابرسی فدرال ، روش اکتاو و تجربه پژوهشگران می باشند.

سوالهای اساسی پژوهش

آیا ایجاد امنیت اطلاعات موجب افزایش اثر بخشی نظامهای اطلاعاتی می شود؟

چند درصد کاربران رایانه‌ها با روش‌های حفاظت اطلاعات آشنایی دارند؟

استفاده اشتراکی از رایانه‌ها، تا چه حد باعث خسارت به اطلاعات پر ارزش سازمان می‌شود؟

تاثیرگذارترین عامل(از بین عوامل انسانی، فیزیکی و فنی) برآسیب‌پذیری سیستمهای اطلاعاتی کدام است؟

سایر سوال هایی که برای شناسایی محیط پژوهش حائز اهمیت هستند

کاربران چگونه پشتیبان تهیه می‌کنند و فایل‌های پشتیبان را کجا نگهداری می‌کنند؟

چه مخاطراتی فناوری اطلاعات سازمان را تهدید می‌کند؟

عوامل موثر در از بین رفتن اطلاعات کدامند؟

عوامل موثر در ارتقای امنیت اطلاعات از دید کاربران کدام است؟

مهارت کاربران در بکارگیری سیستم‌عامل، سیستمهای کاربردی، امنیت سیستم عامل و استفاده از بسته های نرم‌افزاری چه مقدار است؟

آیا کاربران از ارزش اطلاعات موجود در رایانه خود اطلاع دارند؟

آیا کاربران طی سالهای اخیر دوره‌های آموزشی مرتبط با امنیت سیستمهای رایانه‌ای را گذرانده اند؟

روش پژوهش

از نظر محدوده مکانی، پژوهش حاضر در سه سازمان مستقلِ، صرفاً اداری، یک شرکت تجاری و یک سازمان تولید قطعات خودرو اجرا شد. بدلیل حصول نتایج یکسان از تحلیل داده های سه سازمان مورد بررسی، برای اینکه سازمان تولید کننده قطعات از نظر وسعت و تنوع فعالیتهای رایانه ای پوشش مناسبی داشت بر آن شدیم تا نتایج حاصل از تحلیل داده های سازمان مذکور را مورد بررسی قرار می دهیم. اطلاعات لازم در فاصله زمانی فروردین تا خردادماه سال ۱۳۸۵ از طریق پرسشنامه طراحی شده و موجود در شبکه داخلی(وب سایت سازمان) توزیع ونتایج آن در بانک اطلاعاتی ثبت و داده های مورد نیاز گردآوری شد.

جامعه آماری پژوهش حاضر شامل ۵۵ کاربر رایانه اعم از مدیران و کارمندان سازمان مورد مطالعه می باشد که در جمع آوری داده های مورد نیاز، با توجه به کوچک بودن جامعه آماری و امکان دسترسی به آنها از طریق شبکه داخلی و بطور مستقیم، اطلاعات لازم از روش سرشماری گردآوری شد و روش نمونه گیری خاصی مورد استفاده قرار نگرفت. در مجموع با توجه به فرصت زمانی یک ماهه از زمان قراردادن پرسشنامه بر روی وب سایت، از بین ۵۵ کاربر، ۴۸ نفر به سوالات پرسشنامه به صورت کامل پاسخ دادند که تحلیل نتایج بر اساس نظرات این افراد انجام شد. برای افزایش روایی و اعتبار پرسش‌نامه ابتدا پرسش‌نامه به سه تن از کارشناسان امنیت اطلاعات ارایه شد که بعد از نظرخواهی و انجام اصلاحات لازم، شش پرسشنامه نیز بین کاربران توزیع شد (نمونه گیری محدود) و ابهام موجود در رابطه با سوالها مشخص شد و بدین ترتیب پس از شفاف شدن و رفع ابهام از سوال ها، پرسش‌نامه نهایی تهیه شد.

در این پژوهش برای تایید اعتبار پرسش‌نامه، پس از انجام نظر سنجی، داده ها وارد نرم افزار آماری SPSS گردید و ضریب آلفای کرونباخ مورد محاسبه قرار گرفت. باتوجه به آن‌که در سوالها پرسش‌نامه از طیف‌های دو و چند گزینه‌ای استفاده شده، معیار آلفای کرونباخ برای هریک از طیفها مورد محاسبه قرار گرفت که مقدار ضریب آلفا برای سوالهای چند گزینه‌ای برابر ۰/۸۹ و برای سوالهای دو گزینه‌ای برابر ۰/۸۴ بدست آمد که نتایج بدست آمده موید پایائی سوالهای پرسش‌نامه می باشد.

با توجه به اینکه در این پژوهش اطلاعات از روش سرشماری یعنی بررسی کل جامعه آماری بدست آمد، برای تجزیه و تحلیل داده‌ها از روشهای آماری توصیفی نظیر تهیه جداول فراوانی، محاسبه شاخصهای آماری و رسم نمودارهای ستونی استفاده شد.

یافته های پژوهش

داده‌های حاصل از متغیرهای جامعه‌شناختی نشانگر این‌است که ۳۶ در صد کاربران در واحد های صف مشغول فعالیت هستند و ۶۴ در صد در ستاد فعالیت می‌کنند. بیشترین فراوانی سطح تحصیلات مربوط به دیپلم و لیسانس با ۲۷ در صد برای هر یک از واحدهای ستادی و کم‌ترین فراوانی مربوط به فوق‌لیسانس و بالاتر در واحدهای تولیدی با صفر در صد می‌باشد. فراوانی کاربران در واحدهای تولیدی ۱۶ در صد دیپلم، ۱۰ در صد فوق‌دیپلم، ۱۰ در صد لیسانس می‌باشد. ۳۱ در صد کاربران را مدیران عملیاتی و بالاتر تشکیل می‌دهند که اطلاعات مهم و حیاتی زیادی جهت تصمیم‌گیری دراختیار دارند. ۲۵ در صد کاربران رایانه‌های سازمان را کارشناسان تشکیل می‌دهند. این گروه تولیدکنندگان اصلی اطلاعات در سازمان شناخته می‌شوند. ۴۲ در صد کاربران رایانه‌های سازمان را کاربران عادی تشکیل می‌دهند. این گروه از کاربران با بکار گیری نرم‌افزارهای کاربردی و سیستمهای خاص سازمان به ثبت اطلاعات در سرورها می‌پردازند.

هم‌چنین نتایج نظرسنجی به‌ما نشان داد که بیش از ۶۵ در صد پاسخ‌دهندگان دارای سابقه بیش از ۳ سال هستند. بیشترین فراوانی به ترتیب مربوط به کاربران با سابقه بین ۳ تا ۵ سال با ۳۵ در صد می باشد. کاربران با ۱ تا ۳ سال سابقه فعالیت ۱۹ در صد کاربران رایانه را تشکیل می‌دهند. کمترین فراوانی نیز مربوط به کاربران با سابقه کمتر از ۱ سال با ۸ در صد و کاربران با سابقه بیش از ۱۰ سال با ۸ در صد می‌باشد. در بخش دیگری از سوالهای جامعه‌شناختی با عنوان کاربردهای رایانه در سازمان مشخص شد که ۶۱ در صد کاربران به‌عنوان تولیدکننده اطلاعات در زمینه‌های طراحی و ساخت به‌کمک رایانه و ورود اطلاعات نرم‌افزارهای خاص سازمان هستند.

پاسخ به سوالهای پژوهش

پاسخ به سوال اول: آیا ایجاد امنیت اطلاعات موجب افزایش اثر بخشی نظامهای اطلاعاتی می شود؟

به منظور پاسخ به این سوال اساسی پژوهش، سه سوال فرعی مطرح شد. این سوالها در برگیرنده «تاثیر ایجاد و استقرار امنیت اطلاعات بر جلوگیری از سرقت اطلاعات، پیشگیری از تخریب، حذف ویا تغییر اطلاعات» و «عدم انجام دوباره کاری» بود که از کاربران مورد پرسش قرار گرفتند.

نتایج بررسی نشان داد که ۴۷/۹ در صد کاربران کامپیوتر در سازمان، ایجاد سیستم امنیت اطلاعات را در جلوگیری از سرقت اطلاعات سازمان به میزان زیاد و خیلی زیاد و ۲۵ درصد در حد متوسط ارزیابی کرده اند. ۶۰/۴ در صد پاسخ دهندگان معتقدند که تاثیر ایجاد و استقرار امنیت اطلاعات در پیشگیری از تخریب اطلاعات در حد زیاد و خیلی زیاد و ۲۳ در صد در حد متوسط، می باشد همچنین نتایج پاسخها در مورد تاثیر امنیت اطلاعات بر جلوگیری از دوباره کاریها در سازمان نشان می دهد که ۳۹/۶ در صد کاربران این عامل را در حد زیاد و ۵۰ در صد در حد متوسط دانسته اند.

پاسخ به سوال دوم: چند درصد کاربران رایانه‌ها با روشهای حفاظت اطلاعات آشنایی دارند؟

به منظور اندازه‌گیری آشنایی کاربران، از آنها خواسته‌شد میزان اطلاع خود از روش‌های برقراری امنیت اطلاعات مانند روشهای صحیح قرار دادن کلمه عبور، روشهای رمزنگاری اطلاعات، نحوه تهیه پشتیبان به‌موقع و صحیح و هم‌چنین نگهداری صحیح آن را مشخص کنند. پس از جمع‌بندی داده‌های پژوهش مشخص شد ۳۹ در صد کاربران از روش‌های حفاظت اطلاعات آگاهی خیلی کمی دارند، ۳۱ در صد از کاربران آگاهی کمی دارند، ۱۲ در صد آگاهی متوسط، تنها ۲ در صد از کاربران از روشهای حفاظت اطلاعات آگاهی زیادی دارند، ۲ در صد اطلاعی ندارند و ۱۴ در صد به این پرسش پاسخ نداده‌اند. براساس نتایج فوق می‌توان ادعا نمود تنها ۱۴ در صد کاربران در رابطه با حفاظت از اطلاعات سیستمهای رایانه‌ای آگاهی کافی دارند.

پاسخ به سوال سوم: استفاده اشتراکی از رایانه‌ها، تا چه حد باعث خسارت به اطلاعات پر ارزش شرکت می‌شود؟

به‌منظور ارزیابی این سوال، سیستمها به چهارگروه تقسیم شد. گروه اول سیستم‌هایی است که همواره به‌صورت اشتراکی بین کاربران مورد استفاده قرار می‌گیرند و ۳۵ در صد سیستمها را

تشکیل می دهند. گروه دوم سیستمهایی است که اکثر اوقات به‌صورت اشتراکی به‌کار می روند و ۱۲ در صد آنها را تشکیل می دهند. گروه سوم که ۴۲ در صد سیستم‌ها را تشکیل می‌دهند، گاهی اوقات به‌طور مشترک مورد استفاده قرار می‌گیرند. گروه چهارم که تنها یک کاربر دارند و۸ در صد کل رایانه‌های شرکت را تشکیل می‌دهند. یافته های پژوهش نشان داد که طی سال گذشته ۷۰ در صد سیستمهای گروه اول، ۴۷ در صد سیستمهای گروه دوم، ۲۷ در صد سیستمهای گروه سوم و ۱۳ در صد سیستمهای گروه چهارم با یکی از مخاطرات رایج (تغییر، حذف و یا پاک شدن اطلاعات) مواجه شده‌اند.

پاسخ به سوال چهارم: تاثیر گذارترین عامل از بین عوامل انسانی عوامل فیزیکی و تکنیکی بر آسیب‌پذیری سیستمهای اطلاعاتی کدام است؟

برای پاسخ به سوال چهارم، ابتدا سوالها در چهار گروه (مولفه امنیت اطلاعات، مولفه سنجش آگاهی کاربران، مولفه امنیت نیروی انسانی و مولفه امنیت اطلاعات) دسته‌بندی و شاخص آماری جمع امتیازات محاسبه شد. برای محاسبه این شاخص به گزینه خیلی زیاد امتیاز ۵، زیاد ۴، متوسط ۳، کم ۲ و خیلی کم امتیاز ۱ داده شد و با جمع این امتیازها، امتیاز هر سوال بدست آمد. در جدول۲ نتایج عواملی که امنیت اطلاعات سیستمهای رایانه‌ای سازمان را به‌خطر می‌اندازند ارایه شده است. در این جدول مشاهده می‌شود که ویروسهای رایانه‌ای با ۱۰۰ امتیاز و بعد از آن به اشتراک گذاری فایلها با ۷۸ امتیاز بزرگترین تهدید برای اطلاعات سازمان معرفی شده‌اند.

تهدیدات امنیت اطلاعات	امتیازات					شاخص‌های آماری	
	خیلی کم	کم	متوسط	زیاد	خیلی زیاد	جمع امتیازات	میانگین امتیازات
ویروس‌ها	۸	۲۲	۳۰	۲۰	۲۰	۱۰۰	۲/۶۳
اسب‌های تراوا	۱۷	۱٤	۱۵	٤	۵	۵۵	۱/۷۷
نرم افزارهای جاسوسی(مانند ثبت کننده کلید)	۲۰	۱۰	۹	٤	۱۰	۵۳	۱/۷۱
کرم‌های شبکه	۱۸	۱٤	۳	۱۲	۱۰	۵۷	۱/۸٤
اشتراک فایل‌ها	۱۱	۲٤	۲٤	٤	۱۵	۷۸	۲/۲۳
جمع امتیازات						۳٤۳	

جدول ۲- تهدیدهای امنیت اطلاعات

در جدول ۳ میزان آگاهی کاربران براساس عوامل موثر در امنیت اطلاعات سیستمهای رایانه‌ای سنجیده شده‌است. همان‌طور که در جدول مشاهده می‌شود امتیازات گزینه ها به صورت معکوس محاسبه شده است. دلیل آن هم تاثیر معکوس آگاهی کاربران در مقایسه با سایر مولفه‌های امنیت اطلاعات می‌باشد. این درحالی است که سایر مولفه ها تاثیر مستقیم بر امنیت اطلاعات دارند. همانطور که مشاهده می شود بیشترین عدم آگاهی کاربران از امنیت سیستم عامل با ۱۸۴ امتیاز می باشد.

عدم آگاهی کاربران	امتیازات					شاخص‌های آماری	
	خیلی زیاد	زیاد	متوسط	کم	خیلی کم	جمع امتیازات	میانگین امتیازات
سیستم‌عامل	۲	۱۰	٦۳	۳٦	۳۰	۱٤۱	۳/۲۸
سیستم‌های کاربردی	۳	۱٦	٦۹	۲۰	۱۰	۱۱۸	۲/۸۸
امنیت سیستم‌عامل	۱	۱۰	۱۵	٤۸	۱۱۰	۱۸٤	٤/۰۹
بسته‌های نرم‌افزاری	۱۲	۱٤	۳۰	۳٦	۲۵	۱۱۷	۲/۷۲
جمع امتیازات						٥٦۰	

جدول۳ - میزان آگاهی کاربران بر اساس عوامل موثر در امنیت اطلاعات

هر یک از عواملی که در جدول ۴ آورده شده‌اند باعث می‌شوند کاربران حساسیت خود را نسبت به امنیت اطلاعات از دست بدهند. هدف از طرح سوالها، سنجش میزان تاثیر هریک از عوامل موثر در امنیت نیروی انسانی سازمان می‌باشد. همان‌طور که مشاهده می‌شود، پاسخ‌گویان اعلام کرده‌اند که نداشتن مهارت کافی با ۱۴۱ امتیاز بالاترین خطر برای امنیت اطلاعات سازمان می‌باشد و کوتاهی و بی‌مسئولیتی کاربران با ۱۰۰ امتیاز کمترین تهدید برای امنیت اطلاعات سازمان می‌باشد.

عوامل موثر در امنیت نیروی انسانی	امتیازات					شاخص‌های آماری	
	خیلی کم	کم	متوسط	زیاد	خیلی زیاد	جمع امتیازات	میانگین امتیازات
کار زیاد	۸	۲۰	۲۷	٤۰	۱۰	۱۰۵	۲/٦۹
نداشتن مهارت کافی	٦	۱۰	۲۷	٤۸	۵۰	۱٤۱	۳/۳٦
تداخل مسئولیت‌ها	۳	۱۸	۳۹	۳٦	۲۰	۱۱٦	۳/۰۵
عدم اطلاع از میزان ارزش اطلاعات	۳	٦	٤۲	٦٤	۲۰	۱۳۵	۳/۳۸
نداشتن انگیزه	٦	۱٦	۲۷	۲۸	۳۵	۱۱۲	۳/۰۳
کوتاهی و بی‌مسئولیتی	۱۱	۱٤	۲۷	۲۸	۲۰	۱۰۰	۲/٦۳
جمع امتیازات						۷۰۹	

جدول ۴ – عوامل موثر در امنیت نیروی انسانی

جدول ۵ نشان‌دهنده عواملی است که امنیت فیزیکی رایانه‌های سازمان را مورد تهدید قرار می‌دهد. همان‌طور که مشاهده می‌شود، حوادث طبیعی با ۱۱۴ امتیاز بالاترین تهدید امنیت فیزیکی رایانه‌های سازمان را به‌خود اختصاص داده‌است.

عوامل موثر بر امنیت فیزیکی اطلاعات	امتیازات					شاخص‌های آماری	
	خیلی کم	کم	متوسط	زیاد	خیلی زیاد	جمع امتیازات	میانگین امتیازات
حوادث طبیعی مانند سیل،زلزله،صاعقه	۱۵	٤	۱۸	۳۲	٤۵	۱۱٤	۲/۸۵
حوادث غیر طبیعی : اختلالات برق	۸	۱۲	٤۲	۲٤	۲۰	۱۰٦	۲/۷۹
حوادث غیر طبیعی : دمای محیط	۱۷	۱۸	۱۵	۸	۵	٦۳	۱/۸۵
حوادث غیر طبیعی : ترکیدگی لوله آب	۲٤	۸	۹	۸	۵	۵٤	۱/۵۹
ضربات فیزیکی یا لرزش محیط	۱۱	۱۸	۱۲	٤۰	۱۵	۹٦	۲/۵۹
جمع امتیازات						٤۳۳	

جدول ۵ – عواملی که از نظر فیزیکی امنیت رایانه‌های سازمان را تهدید می کند

به‌منظور پاسخ‌گویی به سوال اساسی چهارم ، ابتدا کل داده‌ها جمع‌بندی و شاخصهای آماری جمع و میانگین امتیازات محاسبه شد که در نهایت رتبه‌بندی مخاطرات امنیت اطلاعات به صورت جدول ۶ ارایه شد.

مولفه‌ها	تعداد عوامل	جمع امتیازات	میانگین امتیازات	رتبه‌بندی
عدم آگاهی کاربران	٤	٥٦٠	١٤٠	١
امنیت نیروی انسانی	٦	٧٠٩	١١٨,٢	٢
امنیت فیزیکی	٥	٤٣٣	٨٦,٦	٣
امنیت اطلاعات(تکنیکی)	٥	٣٤٣	٦٨,٦	٤

جدول ۶ – رتبه بندی مخاطرات امنیت اطلاعات

با توجه به این‌که عوامل انسانی که متشکل از دو مولفه آگاهی کاربران و امنیت نیروی انسانی می‌باشد و به‌ترتیب با ۱۴۰ و ۱۱۸/۲ امتیاز بیشترین تاثیر را بر امنیت سازمان می‌گذارد، در نتیجه می‌توان گفت که مولفه امنیت نیروی انسانی بیشترین تاثیر را بر امنیت اطلاعات می‌گذارد. هم‌چنین بررسی به‌ما نشان می‌دهد که امنیت فیزیکی با ۸۶/۶ امتیاز در رتبه سوم مخاطرات قرار دارد و امنیت اطلاعات (تکنیکی) با ۶۸/۶ در رتبه چهارم قرار گرفته‌است.

پاسخ به سوالهای فرعی پژوهش

کاربران چگونه پشتیبان تهیه می‌کنند و فایلهای پشتیبان را کجا نگهداری می‌کنند؟

داده‌های جمع‌آوری شده نشان می‌دهد ۲۵ در صد کاربران همیشه، ۲۵ در صد اکثر اوقات، ۱۵ در صد گاهی اوقات و ۸ در صد به‌ندرت فایل پشتیبان تهیه می‌کنند. ۲۳ در صد کاربران هرگز فایل پشتیبان تهیه نمی‌کنندو۴ در صد نیزهیچ گزینه‌ای را انتخاب نکرده اند. در مجموع می توان گفت حداقل ۲۷ در صد کاربران فایل پشتیبان تهیه نمی‌کنند. ۲۷ در صد کاربران برای نگهداری فایل پشتیبان خود گزینه کپی برروی سایر سیستمهای مجاور را انتخاب کرده‌اند. به‌نظر می‌رسد سهولت دستیابی، کپی و بازیابی اطلاعات در این روش برای کاربران بسیار سریع‌تر از سایر روشها می‌باشد. با توجه به حجم پایین فلاپی و امکان آسیب پذیری زیاد آن از یک طرف و حجم زیاد اطلاعات تولیدی از طرف دیگر، تهیه پشتیبان با استفاده از فلاپی به میزان

بسیار کمی مورد استفاده قرار می گیرد. و به‌همین دلیل این گزینه کمتر انتخاب شده است. کپی فایل روی سی‌دی نیز مراحل متعددی مثل درخواست، تایید درخواست توسط مسئولین، درخواست سی‌دی خام، انتقال فایل به واحد فناوری اطلاعات، رایت سی‌دی و در نهایت انتقال سی‌دی به مرکز درخواست کننده را دارد که از آنها به‌عنوان معضلات تهیه پشتیبان برروی سی‌دی نام برده‌شده است. از موارد فوق این نتیجه حاصل می‌شود که به‌دلیل وجود برخی موانع، اکثر کاربران داده‌های حساس خود را به‌راحتی در اختیار سایرکاربران قرار می‌دهند. این کار ضریب امنیت را به‌شدت کاهش می‌دهد.

چه مخاطراتی فناوری اطلاعات سازمان را تهدید می‌کند؟

نتایج این بررسی حاکی از آن است که ۴۴ در صد کاربران نداشتن سیستم تهیه پشتیبان را مهمترین مشکل ذکر کرده‌اند، ۲۱ در صد وجود ویروسهای رایانه‌ای و ۱۵ در صد نیز خراب‌کاری‌های عمدی یا غیر عمدی سایر کاربران را انتخاب کرده‌اند. ۱۴ در صد نیز به این پرسش پاسخ نداده‌اند.

عوامل موثر در از بین رفتن اطلاعات کدامند؟

پس از جمع بندی داده‌ها و بکارگیری روشهای آماری، مشخص شد از بین رفتن اطلاعات توسط افراد نا آگاه با ۱۵۳ امتیاز، بالاترین خطر می‌باشد. اشتباه غیرعمدی با ۱۳۵ امتیاز دومین عامل خطر از بین‌رفتن اطلاعات در سازمان است. وجود ویروسهای رایانه‌ای و مشکلات فنی سیستمها به‌ترتیب با ۱۱۱ امتیاز و ۹۶ امتیاز عوامل بعدی موثر در از بین رفتن اطلاعات هستند.

عوامل موثر در ارتقای امنیت اطلاعات از دید کاربران کدام است؟

۳۳ در صد کاربران اعتقاد دارند که آموزش مستمر کلید ارتقای سطح امنیتی سازمان می‌باشد، ۴۰ در صد نظارت مستمر، ۱۳ در صد خرید ونصب تجهیزات پیشرفته امنیتی را انتخاب کرده‌اند و ۱۰ در صد معتقد هستند با تشویق و یا تنبیه می‌توان شرایطی را فراهم کرد تا امنیت در سازمان ارتقاء یابد. ۴ در صد از کاربران نیز هیچ گزینه‌ای را انتخاب نکرده‌اند. در توصیف اطلاعات حاصل شده از این پرسش، می‌توان گفت هر اقدامی که بخواهد موجب ایجاد یا ارتقای امنیت اطلاعات شود باید به‌طور مستمر پیگیری شود.

مهارت کاربران در بکارگیری سیستم‌عامل، سیستمهای کاربردی، امنیت سیستم عامل و استفاده از بسته های نرم‌افزاری چه مقدار است؟

با تهیه جداول فراوانی و محاسبه امتیاز هر یک از گزینه ها مشخص شد که کاربران بیشترین مهارت را در استفاده از بسته‌های نرم افزاری با ۱۴۱ امتیاز دارند و پس از آن سیستمهای

کاربردی با ۱۲۷ امتیاز، سیستم‌عامل با ۱۱۷ امتیاز و امنیت سیستم عامل با ۸۶ امتیاز قرار دارند. کمترین مهارت کاربران در امنیت سیستم عامل با ۸۶ امتیاز می باشد و با توجه به این‌که سیستم‌عامل به عنوان واسط بین کاربر، سخت افزار و برنامه‌های کاربردی عمل می‌کند و اهمیت به‌سزایی در استفاده از رایانه ایفا می کند، توجه به آن می‌تواند بر کارآیی و امنیت رایانه تاثیر مستقیم بگذارد. متاسفانه همان‌طور که بیان شد کمترین توجه به امنیت سیستم‌عامل شده‌است و بیشترین توجه به مهارت در به‌کارگیری نرم‌افزارهای کاربردی معطوف بوده‌است. به‌نظر می‌رسد کاربران به‌نوعی موظف به انجام کار با نرم‌افزارهای کاربردی هستند، اما در رابطه با امنیت اطلاعات هیچ‌گونه بازخواستی صورت نمی‌گیرد. به‌همین دلیل می‌توان ادعا کرد کاربران نسبت به امنیت اطلاعات حساسیتی ندارند.

آیا کاربران از ارزش اطلاعات موجود در رایانه خود اطلاع دارند؟

نتایج بررسی ها در مورد آگاهی کاربران از ارزش ریالی اطلاعات موجود روی رایانه آنها نشان داد که ۲۱ در صد گزینه اطلاعی ندارم، ۲۵ در صد خیلی کم، ۲۱ در صد کم، ۱۰ در صد متوسط و ۸ در صد گزینه زیاد و خیلی زیاد را انتخاب کرده‌اند و بنابراین تنها ۸ در صد از ارزش اطلاعات موجود بر روی سیستم رایانه خود مطلع هستند. در این بین ۱۵ در صد پاسخ دهندگان نیز هیچ گزینه‌ای را انتخاب نکرده‌اند.

همان‌طور که در مقدمه مقاله اشاره شد، اطلاعات ارزشمندترین دارایی هر سازمان است. اگر برای سنجش ارزش هر کالا از معیار ارزش ریالی استفاده شود، ارزش آن کالا به راحتی برای همگان قابل درک است. به‌همین منظور ارزش ریالی اطلاعات از دید کاربران مورد بررسی قرار گرفت. همان‌گونه که بیان شد ۸۲ در صد کاربران یا اطلاعی از ارزش اطلاعات موجود در رایانه خود ندارند و یا اطلاع کمی دارند. از این گفته می‌توان نتیجه گرفت که وقتی کاربران از ارزش اطلاعات اطلاعی ندارند، قطعا هیچ تلاشی برای حفظ آن نمی‌کنند.

آیا کاربران طی سال‌های اخیر دوره‌های آموزشی مرتبط با امنیت سیستم‌های رایانه‌ای گذرانده اند؟

نتایج داده های گردآوری شده از کاربران مرتبط با آموزشهای مرتبط با امنیت اطلاعات به‌شکل کلاس، سمینار آموزشی یا سایر روشهای فراگیری، نشان داد که ۴۸ در صد کاربران در طول خدمت خود در رابطه با آشنایی با امنیت سیستمهای رایانه ای دوره‌ای را نگذرانده‌اند. ۲۹ در صد به این سوال پاسخ نداده‌اند، ۱۳ در صد بین یک تا دو سال گذشته دوره دیده‌اند، ۸ در صد بیش از سه سال گذشته، ۲ در صد بین دو تا سه سال گذشته و متاسفانه طی سال گذشته هیچ یک از پاسخ‌گویان در هیچ دوره‌ای شرکت نکرده‌اند.

در تفسیر اطلاعات بالا فقط می‌توان ابراز تاسف کرد. زیرا تحولات در حوزه فناوری اطلاعات بسیار سریع رخ می‌دهد. با توجه به داده‌های کسب شده می‌توان نتیجه گرفت اندک دانایی موجود در کاربران مربوط به گذشته است و نمی‌تواند کمک موثری در حفظ اطلاعات سازمان نماید.

خلاصه ای از فرصت‌ها و تهدیدهای موجود به‌واسطه جمع‌آوری، دسته‌بندی و تحلیل داده‌های پرسش‌نامه کسب شده‌است، در ادامه آورده می شود. بدیهی است که اگر از یک فرصت درست استفاده نشود، می‌تواند تبدیل به تهدید شود. از این‌رو براساس منافع و دارایی‌های اطلاعاتی سازمان، تقسیم‌بندی زیر صورت گرفته‌است.

فرصت ها

- سطح تحصیلات ۳۱ در صد کاربران لیسانس و بالاتر هستند.
- اطلاعات اصلی سازمان (نقشه های فنی، مکاتبات اداری، اطلاعات مالی و...) تماماً توسط رایانه جمع‌آوری، پردازش وتوزیع می‌گردند.

تهدیدها

- نداشتن سیستم مناسب تهیه پشتیبان یکی از مهمترین تهدید ها شناسائی گردید.
- نگهداری اطلاعات حساس سازمان بر روی رایانه های شخصی(PC)
- استفاده اشتراکی از رایانه
- عدم آگاهی کاربران از ارزش اطلاعات در دسترس(عدم آگاهی از ارزش اطلاعات باعث می‌شود تولیدکنندگان و استفاده‌کنندگان از اطلاعات حساسیتی نسبت به حفظ آن نداشته‌باشند)
- عدم آگاهی کافی کاربران از روشهای حفظ اطلاعات.

نتیجه‌گیری

باتوجه به این‌که دغدغه اصلی کارکنان برآورده ساختن درخواستها و انجام وظایفی است که بر عهده آنها می باشد اولین چیزی که معمولاً نادیده گرفته می‌شود مسائل امنیتی است. دلیل عمده آن را می توان نداشتن قانون مدون و ابلاغ شده به کارکنان دانست. نکته بسیار مهم این‌است که، نداشتن مقررات مکتوب باعث می شود اولا کارکنان ندانند چه وظایفی نسبت به حفظ اطلاعات سازمان دارند و ثانیا در صورت بروز تخلف آنها، مرجعی برای رسیدگی به تخلفات وجود ندارد.

همچنین نظرسنجی نشان می‌دهدکه باتوجه به نقاط ضعف بسیار زیاد سازمان درحفظ

داراییهای‌اطلاعاتی خود، بایستی با پیاده‌سازی سیستم مدیریت امنیت اطلاعات، ابتدا داراییهای حیاتی خود را شناسایی کنند و پس از آن مخاطرات هر یک را مشخص کنند. در ادامه نیز با کنترل هر یک از مخاطرات روشهایی را برگزیند تا به‌کمک آن مخاطرات به حداقل رسانده‌شود. به عبارت دیگر با پیاده سازی سیستم مدیریت امنیت اطلاعات می توان شرایطی را فراهم کرد تا مدیران، کارشناسان و کاربران بدون دغدغه به فعالیت‌های اصلی خود ادامه دهند.
براساس مطالعات انجام شده شرط موفقیت سیستم مدیریت امنیت اطلاعات، استمرار چرخه امنیت اطلاعات است که هم در استاندارد انگلیسی BS و هم در شیوه GAO بر آن تاکید شده‌است. اگر استمرار چرخه امنیت اطلاعات کم‌رنگ شود، به جرات می‌توان ادعا کرد سیستم مدیریت امنیت اطلاعات در سایر مشغله‌های مدیران و کاربران محو خواهد شد. از این رو ایجاد تشکیلات امنیت اطلاعات، انتخاب مدیر امنیت اطلاعات و نظارت مستمر مدیر ارشد سازمان از ارکان اساسی برقراری امنیت اطلاعات در هر سازمان می‌باشد.

پی نوشت ها

1 . Commercial Computer Security Center
2 . Users Code of Practice
3 . Information Security Management System
4 .Code of Practice for Information Security Management
5 . Information Security Management System
6 . General Accounting Office
7 . Risk Management Principles
8 . Carnegie Mellan

۹. پروفسور مت بیشاب استاد دانشگاه کالیفرنیا می باشد. او تحقیقات بسیاری بر روی آسیب پذیری های فناوری اطلاعات ، امنیت سیستم های نرم افزاری ، شبکه های کامپیوتری و طراحی مدل های امن انجام داده است.

10. National Institute of Standards and Technology (NIST)
11 . Sadowsky
12 . Wold
13. Hone and Eloff
14 . Callio

شرکت کالیو یکی از معتبرترین موسسات ارائه دهنده مشاوره و گواهی نامه سیستم مدیریت امنیت) (اطلاعات در جهان می باشد

۱۵- دو نوع سیاست امنیتی داریم ۱- سیاست امنیتی BS7799 با توجه به فضای حاکم بر استاندارد کلان ۲- سیاست امنیتی جزئی که به سیاست امنیتی سطح دو معروف است

منابع فارسی

رادرجبی، مهدی.(۱۳۸۵) **مطالعه سیستم‌های مدیریت امنیت اطلاعات و ارایه شاخص و الگو برای سازمان‌ها**، پایان نامه کارشناسی ارشد دانشگاه صنعتی مالک اشتر، تهران.

خاکی،غلامرضا. (۱۳۷۸). **روش تحقیق با رویکردی در پایان‌نامه‌نویسی چاپ دوم ،تهران**: انتشارات بازتاب:

خالقی، محمود. (۱۳۸۳). **راهنمای پیاده سازی سیستم مدیریت امنیت اطلاعات**. تهران: دبیرخانه شورای‌عالی فضای تبادل اطلاعات کشور.

میوالد، اریک. (۱۳۸۳). **امنیت شبکه‌های کامپیوتری**، ترجمه سید احمد صفایی چاپ اول ،تهران : نشر دانش پرور،.

کریم بیگی، آرش.۱۳۸۴. **ساخت و پیاده‌سازی یک سیاست امنیتی موفق**. تهران: دانشگاه صنعتی مالک اشتر

منابع لاتین

Alberts, C and Dorofee, A.(2001). **Introduction to the OCTAVE Approach.** Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University,. Available at http://www.cert.org/octave.

British standard institute.(1999). Information security management – part1: **Code of Practice for information security management** (BS7799-1) ;

British standard institute(1999). Information security management – part 2: **Specification for information security management system** (BS7799-2)

Bishop, M. (2003)**.what is security?** Position Paper for the Workshop on

Education in Computer Security, Monterey, CA. http://computer.org/security/2003/what is security.pdf

General Accounting Office(1998) . Executive Guide; Information Security Management, Learning From Leading Organizations (GAO/AIMD-98-68, May 1998). www.gao.org

Hone, K & Eloff, J.(2003). **What Makes an Effective Information Security Policy?** Network Security; Available at http://www.sciencedirect.com

International Standard Organization; Information Technology.(2000). **Code of practice for information security management** (ISO/IEC17799);

International Standard Organization; Information Technology – **Guidelines for the management of IT security** – Part 1 – part5 (ISO/IEC TR 13335)

Bisson,J. (2004), **The BS** 7799 / **ISO 17799 Standard For a better approach to information security**،Callio Technologies [13]. http://www.ndc.ir/rulles.php (1384/06/22)

Japan Information Processing Development Corporation . (2004). **How to Establish an ISMS Management Framework** ، http://www.isms.jipdec.

National Institute of Standard and Technology (NIST).(1995). **An Introduction to Computer Security: The NIST Handbook**. Special Publication800-12. http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Sadowsky ,G . et al (2003) **IT Security Handbook** . infoDev. Worldbank.

Wold, G.(2004) **Key factors in making Information Security Policies effective;** Available at http://cran.us.r-project.org/