دانشگاه سیستان و بلوچستان
تحصیلات تکمیلی

پایان نامه کارشناسی ارشد

مدیریت فناوری اطلاعات گرایش کسب و کار الکترونیک

عنوان:

مطالعه کنترل‌های امنیت اطلاعات براساس استاندارد های بین المللی

استاد راهنما:

دکتر مهدی کاظمی

استاد مشاور:

دکتر نورمحمد یعقوبی

تحقیق و نگارش:

حمید خواجویی

بهمن ۱۳۹۰


بسم الله الرحمن الرحيم

بسمه تعالی

این پایان نامه با عنوان **مطالعه کنترل های امنیت اطلاعات بر اساس استاندارد های بین المللی** قسمتی از برنامه آموزشی دوره کارشناسی ارشد **مدیریت فناوری اطلاعات** توسط دانشجو **حمید خواجویی** تحت راهنمایی استاد پایان نامه **دکتر مهدی کاظمی** تهیه شده است. استفاده از مطالب آن به منظور اهداف آموزشی با ذکر مرجع و اطلاع کتبی به حوزه تحصیلات تکمیلی دانشگاه سیستان و بلوچستان مجاز می باشد.

حمید خواجویی

این پایان نامه ..... واحد درسی شناخته می شود و در تاریخ ..... توسط هیئت داوران بررسی و درجه ..... به آن تعلق گرفت.

	نام و نام خانوادگی	**امضاء**	**تاریخ**
استاد راهنما:			
استاد راهنما:			
استاد مشاور:			
داور ۱:			
داور ۲:			
نماینده تحصیلات تکمیلی:			

دانشگاه سیستان و بلوچستان

تعهدنامه اصالت اثر

اینجانب حمید خواجویی

تأیید می کنم که مطالب مندرج در این پایان نامه حاصل کار پژوهشی اینجانب است و به دستاوردهای پژوهشی دیگران که در این نوشته از آن استفاده شده است مطابق مقررات ارجاع گردیده است. این پایان نامه پیش از این برای احراز هیچ مدرک هم سطح یا بالاتر ارائه نشده است. کلیه حقوق مادی و معنوی این اثر متعلق به دانشگاه سیستان و بلوچستان می باشد.

نام و نام خانوادگی دانشجو: حمید خواجویی

امضاء

تقدیم به پدرم

کوهی استوار و حامی من در طول تمام زندگی

تقدیم به مادرم

سنگ صبوری که الفبای زندگی به من آموخت

تقدیم به همسرم

که در سایه همیاری و همدلی او به این منظور نائل شدم.

سپاسگزاری

به مصداق «من لم یشکر المخلوق لم یشکر الخالق » بسی شایسته است از اساتید فرهیخته و فرزانه جناب آقایان دکتر مهدی کاظمی و دکتر نور محمد یعقوبی که با کرامتی چون خورشید ، سرزمین دل را روشنی بخشیدند و گلشن سرای علم و دانش را با راهنمایی های کار ساز و سازنده بارور ساختند، تقدیر و تشکر نمایم.

همچنین جا دارد که از زحمات جناب آقای مهندس حمید ولی و آقای هاشم نصرآبادی که در مراحل اجرای پایان نامه کمک های بسیاری نمودند، تشکر نمایم.

چکیده

در طی سال ها، سازمان ها زیان های سیستمی بسیاری را تجربه کرده اند که این زیان ها تاثیر مستقیمی بر ارزشمند ترین دارایی آنها یعنی اطلاعات داشته است. دستیابی به امنیت اطلاعات، با پیاده سازی مجموعه ای از کنترل های مناسب از جمله خط مشی ها، فرایند ها، رویه ها، ساختار سازمانی و فعالیت های نرم افزاری و سخت افزاری میسر می شود. از طرفی فرایند شناسایی و انتخاب موثرترین کنترل های امنیت اطلاعات در سازمان ها در گذشته به صورت چالشی بزرگ بوده است و تلاش‌های بسیاری در جهت رفع این مشکل از طریق استفاده از موثرترین روش ممکن صورت پذیرفته است. اهداف این پژوهش عبارتند از اولویت بندی حوزه های مدیریتی و اهداف کنترلی امنیت اطلاعات بر اساس استاندارد مدیریت امنیت اطلاعات ایزو ۲۷۰۰۱، که برای این منظور از روش تحلیل سلسله مراتبی فازی استفاده شد. جهت گردآوری داده های تحقیق از پرسشنامه ای مشتمل بر ۱۴۴ مقایسه زوجی استفاده شد. جامعه این تحقیق مناطق چهارگانه شرکت ملی پخش فرآورده های نفتی ایران در منطقه شرق و جنوب شرق کشور که عبارتند از کرمان، زاهدان، خراسان جنوبی و چابهار بوده که به دلیل محدود بودن تعداد اعضای کمیته های راهبری این چهار منطقه، از روش سرشماری در نمونه گیری استفاده شد. بعد از تجزیه و تحلیل داده ها ضریب ناسازگاری ۰.۰۵برای پرسشنامه های تحقیق بدست آمد که این مقدار کمتر از ۰.۱ بوده و مقدار قابل قبولی می باشد. نتایج حاصل از تحقیق حاکی از آن است که حوزه های مدیریتی کنترل دسترسی و اکتساب، بهبود، حفظ و نگهداری سیستم های اطلاعاتی به ترتیب با اوزان محلی ۰.۱۲۴ و ۰.۱۲۱ اولویت های اول و دوم و مدیریت دارائی با وزن محلی ۰.۰۳۶ اولویت آخر را در میان ۱۱ حوزه تحقیق به خود اختصاص دادند. همچنین در میان اهداف کنترلی، مدیریت دسترسی کاربر و مدیریت تحویل خدمت شخص سوم به ترتیب با اوزان جهانی ۰.۰۴۷ و ۰.۰۰۷، اولویت های اول و آخر را در میان ۳۹ هدف کنترلی امنیت به خود اختصاص دادند.

کلمات کلیدی: مدیریت امنیت اطلاعات، استاندارد ایزو ۲۷۰۰۱، تحلیل سلسله مراتبی فازی، کنترل های امنیت اطلاعات.

فهرست مطالب

لیست جداول

لیست نمودارها

لیست شکل ها

فصل اول

کلیات تحقیق

۱-۱- مقدمه

استفاده گسترده سازمان‌های قرن بیست و یکم از فناوری اطلاعات منجر به تحولات عظیمی در ساختار کسب و کار آن‌ها شده است. اما فناوری اطلاعات نیز همانند سایر تکنولوژی‌ها، ظرافت‌ها و نکات خاصی را به همراه دارد، که عدم توجه به آن‌ها، استفاده بهینه از این فناوری را تحت تاثیر قرار داده و حتی ممکن است سازمان را با تهدید یا چالش‌هایی روبرو سازد. امروزه یکی از مهمترین ابعاد فناوری اطلاعات، امنیت آن می‌باشد. آمار روزافزون هک شدن و نفوذ به وب‌سایت‌ها، افشای اطلاعات محرمانه، انتشار ویروس‌ها و کرم‌های رایانه‌ای، جاسوسی و خرابکاری رایانه‌ای، جعل هویت و دسترسی غیرمجاز و بسیاری از تهدیدات دیگر، هشداری برای توجه سازمان‌ها به این مقوله است. عدم پرداختن به امنیت اطلاعات ممکن است تبعاتی برای کسب و کار داشته باشد که جبران آن ماه‌ها و سال‌ها به طول بینجامد. یکی از مسائلی که می‌تواند حیات و برتری سازمان‌ها را در محیط پر ریسک و رقابتی حفظ کند، توانایی امنیتی این سازمان‌ها در مقابله با تهدیدات فضای مجازی می‌باشد(همکاران سیستم, ۱۳۹۰). به عبارت دیگر مدیریت دارایی های اطلاعاتی که هر روز در حال رشد هستند در تمام دنیا به چالشی برای تمامی افراد و شرکت های بزرگ تبدیل شده است. در واقع امنیت فناوری اطلاعات به عنوان مهم ترین چالش بر سر راه گسترش این فناوری محسوب می شود(رضوانی چمن زمین, ۱۳۸۳).

دستیابی به امنیت اطلاعات، با پیاده سازی مجموعه ای از کنترل های مناسب از جمله خط مشی ها، فرایند ها، رویه ها، ساختار سازمانی و فعالیت های نرم افزاری و سخت افزاری میسر می شود. این کنترل ها در موارد لازم باید مستقر، پیاده سازی، پایش، بازبینی و اصلاح شده تا از برآورده شدن اهداف خاص امنیتی و کسب و کار در سازمان اطمینان حاصل شود. بنابراین سازمان ها بایستی راههایی پیدا می کردند تا اطمینان حاصل کنند که مناسب ترین و موثر ترین کنترل های امنیت اطلاعات در جهت حفاظت از مهم ترین و حیاتی ترین اطلاعات طبقه بندی شده آنها پیاده سازی شده اند.

۱-۲- مسأله تحقیق

حفاظت از اطلاعات برای سازمان ها از اهمیت بسیار بالایی برخوردار است. در طی سال ها، سازمان ها زیان های سیستمی بسیاری را تجربه کرده اند که این زیان ها تاثیر مستقیمی بر ارزشمند ترین دارایی آنها یعنی اطلاعات داشته است(Otero, Otero, & Qureshi, 2010). نود درصد سازمانها معتقدند امنیت اطلاعات برای دستیابی آنها به اهداف کلی شان بسیار حائز اهمیت است و طی تحقیقی یک سوم از سازمانهای مورد ارزیابی بیان داشته اند که یک نقص امنیتی بزرگ می تواند آنها را از صحنه تجارت خارج سازد. طی تحقیقی دیگر ۲۰٪ از مصرف کنندگان بیان داشته اند که بعد از آگاهی از یک نقص امنیتی در سازمان، ارتباطشان را با آن سازمان پایان داده اند و ۵۸٪ از پاسخ دهندگان بیان داشته اند که نقص امنیتی در یک سازمان باعث می شود تا آنها اعتمادشان را به سازمان مربوطه از دست بدهند(ابرار اقتصادی, ۱۳۸۷). با این وجود بر اساس تحقیق جهانی امنیت اطلاعات ارنست و یانگ[1] در سال ۲۰۰۳ بیش از ۳۴ % از سازمانها اظهار کرده اند که قدرت کافی برای تشخیص اینکه آیا سیستمهایشان درحال حاضر مورد حمله قرار دارند یا خیر را ندارند و بیش از ۳۳ % اظهارکرده اند که قادر به ارائه عکس العمل مناسب در واکنش به رخدادهای امنیتی نیستند. نتایج تحقیقی دیگر در سال ۲۰۰۴ بیانگر آن بود که هفتاد درصد سازمان ها حداقل یک مرتبه مورد تهاجم قرار گرفته اند(دهقان نیری, ۱۳۸۷). تحقیقی دیگر در سال ۲۰۰۵ نشان داد، عواملی که امنیت کامپیوترها را مورد تهدید قرار میدهند از جمله ویروس ها، کرم ها و اسب های تروجان در آن سال ۴۸٪ نسبت به سال پیش افزایش یافته اند(ابرار اقتصادی, ۱۳۸۷).

آماری دیگر در سال ۲۰۰۶ که توسط سازمان جهانی امنیت اطلاعات ارائه شد بیان گر آن بود که بیش از ۶۴٪ از سازمانها در سراسر جهان فاقد جایگاه های شغلی در زمینه امنیت اطلاعات می باشند. همچنین تنها ۳۷٪ از سازمان ها دارای استراتژی امنیتی می باشند(PWC, 2011). این درحالی است که سه پنجم از سازمان ها بیان نموده اند که یافتن نقص های امنیتی برایشان مشکل می باشد(موسسه استاندارد و تحقیقات صنعتی ایران, ۱۳۸۶)، و ۷۲٪ بیان نموده اند که در مورد امنیت اطلاعات و یا امنیت فیزیکی دارایی هایشان ، دچار نگرانی می باشند. نتایج تحقیقاتی دیگر در این سال بیانگر آن بود که از میان هر سه کاربر کامپیوتر یکی قربانی ویروس ها،جاسوس افزارها

[1] Ernst & young

یا فیشینگ[1] شده اند. مصرف کنندگان آمریکایی در عرض دو سال ۷/۸ میلیون دلار برای تعمیر و یا تعویض قطعات کامپیوتری بخاطر حملات سوء افزار هزینه دادند و از میان هر۲۰ پست الکترونیکی یکی آلوده به سوء افزار می باشد. همچنین به طور میانگین ضرر وارده به هـر قربـانی فیشـینگ از ۲۵۷ دلار در سـال ۲۰۰۵ بـه ۱۲۴۴ دلار در سـال ۲۰۰۶ افزایش یافته است(ابرار اقتصادی, ۱۳۸۷).

طی بررسی صورت گرفته در سال ۲۰۰۷ نیز ۸۵٪ از سازمانهای مورد بررسی گزارش داده اند که مشکل امنیتی داشته اند این در حالی است که به طور متوسط هزینه ابزارهای جلوگیری کننده چهار برابر کمتر از هزینه یک نقص امنیت می باشد. این آمارها حاکی از آن است که همه سازمانها – چه کوچک و چه بزرگ - فشارهای مالی و روانی تهدیدهای امنیت فناوری اطلاعات را حس می کنند(موسسه استاندارد و تحقیقات صنعتی ایران, ۱۳۸۶).

با توجه به گستردگی و ناهمگونی فناوری در لایه های مختلف سیستم هـای اطلاعـاتی، بـه کـارگیری سیسـتم مدیریت امنیت اطلاعات جهت هدف بخشی، تضمین یکپارچگی و هماهنگی فعالیت های انجام شده به منظـور نیـل به اهداف امنیت تدوین شده در راستای اهداف کسب و کار سازمان ها و تضمین رشد و بقاء سیستم امنیت اطلاعات را به یک الزام مبدل ساخته است(نشریه ارتباطات, ۱۳۸۹).

با توجه به آمار و اطلاعات ارائه شده در مورد مشکلات امنیتی سازمان نیاز است تا سطح قابـل قبـولی از امنیـت اطلاعات را در سازمان ها بر قرار سازیم. یک سطح قابل قبول امنیت اطلاعات می تواند تنها در حالتی ایجاد شود که مجموعه صحیحی از کنترل های امنیتی(در هر دو بعد رویه ای و فنی) در قالب پیاده سازی استاندارد های مـدیریت امنیت اطلاعات، شناسایی، اجرا و نگهداری شوند(Von Solms, 1998).

همان طور که گفته شد دستیابی به امنیت اطلاعات، با پیاده سازی مجموعه ای از کنترل های مناسب از جملـه خط مشی ها، فرایند ها، رویه ها، ساختار سازمانی و فعالیت های نرم افزاری و سخت افزاری میسـر مـی شـود. ایـن کنترل ها در موارد لازم باید مستقر، پیاده سازی، پایش، بازبینی و اصلاح شـده تـا از بـرآورده شـدن اهـداف خـاص امنیتی و کسب و کار در سازمان اطمینان حاصل شود. پس از اینکه نیاز های امنیتی و ریسک ها، شناسایی شـدند و تصمیم برای برطرف سازی ریسک ها اتخاذ گردید، کنترل های مناسب باید به نحوی انتخاب و بکار گرفته شوند، تـا از کاهش ریسک ها و رسیدن به حد قابل قبول، اطمینان حاصل شـود. انتخـاب کنتـرل هـای امنیتـی، بسـتگی بـه

[1] Phishing

تصمیمات سازمان دارد که بر اساس معیار پذیرش ریسک، گزینه های برطرف سازی ریسک و رویکرد مدیریت ریسک در سازمان و همچنین کلیه قوانین و مقرارات ملی و بین المللی که باید مد نظر قرار گیرد اتخاذ می شود(Otero et al., 2010).

نفت مهمترین منبع درآمد کشور می باشد. با استفاده روز افزون از فناوری اطلاعات و برخط شدن بسیاری از خدمات ارائه شده از سوی دستگاههای دولتی و خصوصی، شرکت ملی پخش فرآورده های نفتی ایران نیز از این قافله عقب نمانده و بسیاری از خدمات خود را از طریق اینترنت به مشتریان عرضه می کند. از جمله این خدمات می توان به سایت های ثبت سفارش و خرید فرآورده های نفتی اشاره نمود که چندین سال است مورد استفاده عموم قرار میگیرند. بعد از حمله ویروسی کامپیوتری به تاسیسات اتمی ایران، توجه به بحث امنیت اطلاعات بیشتر شد و اجرای پروژه های این حوزه سرعت گرفت که شرکت ملی پخش فرآورده های نفتی ایران نیز از این قاعده مستثنی نیست. تاکنون در زمینه امنیت تنها به سخت افزار و نرم افزار توجه می شد اما هم اکنون این تفکر جای خود را به تفکر پیاده سازی سیستم مدیریت امنیت اطلاعات که مباحث مدیریتی را نیز به دو حوزه قبلی افزوده، داده است. به دلیل گستردگی فعالیت های شرکت ملی پخش فرآورده های نفتی ایران، شناسایی و پیاده سازی کنترل های مناسب در شرکت مذکور و عدم اعمال کنترل های غیر ضروری، نقش بسیار مهمی در کاهش هزینه و زمان و بهبود نتیجه پیاده سازی این سیستم دارد. لذا در این پژوهش به دنبال پاسخ به این سوالات هستیم که از دیدگاه اعضای کمیته های راهبری جامعه مورد مطالعه، کدام حوزه های مدیریتی در برقرار نمودن یک سیستم امن اطلاعاتی، اولویت بیشتری داشته و وزن آنها به چه میزان است و همچنین کدام اهداف کنترلی در برقرار نمودن یک سیستم امن اطلاعاتی، اولویت بیشتری داشته و وزن آنها به چه میزان است.

۱-۳- ضرورت انجام تحقیق

با توجه به وضعیت نامطلوب امنیت فضای تبادل اطلاعات کشور به ویژه در حوزه دستگاه های دولتی و خصوصی در چند سال اخیر تعدادی از سازمان های داخلی برای مقابله با این مشکلات اقدام به اجرای سیستم مدیریت امنیت اطلاعات نموده اند(ابرار اقتصادی, ۱۳۸۷). اما تنها ۱۲ سازمان موفق به دریافت گواهینامه ISMS شده است. این در حالی است که تعداد سازمان هایی که در جهان موفق به اخذ گواهی مدیریت امنیت اطلاعات شده اند به ۷۲۰۵

سازمان رسیده است و هر ساله نیز بر تعداد این سازمان ها افزوده می گردد(International register of ISMS certificates, 2011). همچنین در سند راهبردی امنیت فضای تبادل اطلاعات کشور، پیاده سازی سیستم مدیریت امنیت اطلاعات بعنوان یکی از اقدامات اساسی برای راهبردهای امن سازی زیرساختهای حیاتی کشور در قبال حملات الکترونیکی و ایجاد و توسعهٔ نظامهای فنی فرابخشی افتا[1] در نظر گرفته شده است که اجرای آن باید توسط تمام سازمانهای دولتی مد نظر قرار گیرد. ایجاد اعتماد در مشتریان و ارباب رجوع، ایجاد شفافیت، قابلیت پیگیری و حسابرسی، کاهش ریسک های فنی، مالی، حقوقی و قضایی امنیت فضای تبادل اطلاعات، جلوگیری از حملات و دسترسی های غیر مجاز ناشی از عدم رعایت مسائل امنیتی، مهار خسارت های ناشی از ناامنی، تامین محرمانگی، صحت و قابلیت دسترسی برای ارتباطات، اطلاعات، نرم افزارها و سخت افزارها همگی از مزایای پیاده سازی این سیستم به شمار می روند و سازمان ها را بر آن می دارند تا اقدام به اجرای این سیستم نمایند(بزرگمهر, ۱۳۸۴).

مدیر عامل شرکت فناوری اطلاعات نیز در مصاحبه ای اعلام نمود بر اساس مصوبه دولتی تمامی دستگاه های اجرایی مشمول ماده پنج قانون خدمات کشوری ملزم به پیاده سازی سامانه سیستم مدیریت امنیت اطلاعات هستند و می بایست تا پایان سال ۹۰ این گواهی را دریافت کرده باشند. هیات وزیران شرکت فناوری اطلاعات ایران را مسئول بررسی و ممیزی این استاندارد نمود(نشریه ارتباطات, ۱۳۸۹).

بنابراین می توان دریافت که ناگزیر به پیاده سازی سیستم مدیریت امنیت اطلاعات در سازمان های دولتی و خصوصی در کشور خود هستیم. در پیاده سازی سیستم مدیریت امنیت اطلاعات پس از این که نیاز های امنیتی و ریسک ها، شناسایی شدند و تصمیم برای برطرف سازی ریسک ها اتخاذ گردید، کنترل های مناسب باید به نحوی انتخاب و بکار گرفته شوند، تا از کاهش ریسک ها و رسیدن آنها به حد قابل قبول، اطمینان حاصل شود(ابرار اقتصادی, ۱۳۸۷). سازمان ها بایستی راههایی پیدا می کردند تا اطمینان حاصل کنند که مناسب ترین و موثر ترین کنترل های امنیت اطلاعات در جهت حفاظت از مهم ترین و حیاتی ترین اطلاعات طبقه بندی شده آنها پیاده سازی شده اند.

[1] امنیت فضای تبادل اطلاعات