به نام آن که جان را فکرت آموخت

وزارت علوم، تحقیقات و فناوری

دانشکده مدیریت

پروژه کارشناسی رشته مدیریت بازرگانی

عنوان:

بررسی و مطالعه ی نقش مدیریت ریسک در سیستم های فناوری اطلاعات

(مورد پژوهی: فروشگاه پویان کامپیوتر)

استاد راهنما:

جناب آقای مهندس مسعود نصر اصفهانی

پژوهشگر:

آرش احمدی اصفهانی

سال ۱۳۸۷

قدردانی

به این وسیله از راهنمایی های ارزشمند جناب آقای مهندس نصر اصفهانی سپاس گزاری می شود.

تقدیم به علاقه مندان دانش مدیریت و فناوری اطلاعات

چکیده

تهیه‌ی این پژوهش با هدف بررسی نقش ابزارها و استراتژی های مدیریت ریسک در سیستم های فناوری اطلاعات برای کاهش ریسک در فروشگاه پویان کامپیوتر بوده است.

در این تحقیق از روش های جست و جو در اینترنت و منابع کتابخانه ای برای ادبیات تحقیق و در بخش گردآوری اطلاعات تحقیق از روش میدانی با استفاده از نرم افزار Expo-Se و ابزارهای مصاحبه و مشاهده استفاده شده است. همچنین با توجه به مطالب ادبیات تحقیق و تجزیه و تحلیل اطلاعات موارد زیر نتیجه گیری می شود: ۱- نقش فناوری اطلاعات در کاهش ریسک به این شرح است: با به کارگیری نظام های پیشرفته علوم رایانه ای و خدمات، به دلیل سرعت و دقت آن ها، ریسک و هزینه معاملات کاهش یافته است. کاهش هزینه ها به علت کاهش هزینه های ناشی از جست و جو، انتخاب، نظارت، هماهنگی و سرعت انتقال اطلاعات می باشد. ۲- نصب تجهیزات ایمنی برای سیستم های کامپیوتر و همچنین سیستم اطفای حریق باعث شده اند تا از ریسک های منفی (زیان آور) جلوگیری شود. ۳- تجهیزات و امکانات آموزشی فروشگاه پویان کامپیوتر به صورت کتاب ها و مقاله های الکترونیکی در پایگاه اطلاعات آن در دسترس مدیران و کارکنان است که ماهانه به دفعات بسیاری به روز می شوند. ۴- خدمات و فعالیت های این فروشگاه برای استفاده تجهیزات در ریسک بلند مدت به صورت مرحله ای و فرآیندی می باشد. به این صورت که ابتدا نحوه ی کاربرد تجهیزات به مدیران و کارکنان آموزش داده شده سپس آن تجهیزاتی که در ارتباط با موضوع ریسک هستند گردآوری شده و مورد استفاده قرار می گیرند. ۵- بخش های مختلف فروشگاه در کاهش یا حفظ هزینه های مالی و افزایش منافع مادی برای سازگاری با یکدیگر و محیط اطراف خود و ماتریس های احتمال- اثر، ریسک ها را در درآمدها و هزینه های فروشگاه ارزیابی می کنند.

فهرست مطالب

فصل اول: کلیات پژوهش

۱-۱- مقدمه

پیشگیری از خسارات یا حادثه، رفتاری کاملاً متکی بر اندیشه است و فقط در سازمانی مؤثر است که از بالای هرم سازمانی اجرا شود. ریسک به معنای بی اطمینانی در مورد پیامدهای حادثه مورد انتظار است. ریسک مهم تر از آن است که تنها به یک مدیر ریسک سپرده شود، مدیریت ریسک را نباید همپای دیگر مدیرانی فرض کرد که مسئولیت ها و وظایف مختلف دارند. وی باید مدیریت فیزیکی ریسک را اعمال کرده و با بخش های خدماتی، بازرگانی و غیره در ارتباط نزدیک و هماهنگ باشد.

۱-۲- بیان مسأله

امروزه شرکت ها در محیط پیچیده و متغیری فعالیت می کنند. در این شرایط شرکت ها برای دستیابی به هدف های خود و کاهش نوسان های نامطلوب، برای مدیریت ریسک هایی که با آن مواجه هستند، اهمیت زیادی قایل هستند. شرکت ها با ریسک های بزرگی مانند ریسک بازار (مانند ریسک نرخ ارز، نرخ بهره و قیمت سهام)، ریسک نقدینگی، ریسک اعتباری و ریسک عملیاتی (مانند ریسک فناوری اطلاعات، نیروی انسانی و قانون ها) رو به رو هستند.

راه کارهای مدیریت ریسک در بقا و سودآوری به شرکت کمک کند. مدیریت ریسک می تواند به طور موفقیت آمیزی توسط سازمان ها، دولت های محلی و خانواده ها به کار برده شود. مدیریت ریسک تا اندازه ای یک گزینه نیست. اگر ریسک ها نادیده گرفته شوند، روش اشتباهی در مدیریت ریسک انتخاب شده است که فقط به صورت شانسی ممکن است بهترین روش باشد. سازمان ها با مدیریت درست این ریسک ها قادر به دستیابی به نتایج قابل قبول با حداقل هزینه خواهند بود. اکثر سازمان ها اهمیت فزاینده مدیریت ریسک را تشخیص داده اند. به موازات پیچیده تر شدن زندگی بشر توسعه و ارتباطات و افزایش عدم اطمینان، ریسک های جدیدی نیز خلق شده اند و شدت بسیاری از ریسک های بالای سازمان مسئولیت ریسک را به یک بخش خصوصی اختصاص داده اند. در اکثر کشورهای بزرگ و بسیاری از انواع سازمان های کوچکتر مدیریت هر جا که آینده ناشناخته باشد ریسک وجود دارد که تحت عنوان انحراف در پیشامدهای ممکن آینده تعریف می شود و در نتیجه اگر حداقل دو پیشامد ممکن باشد ریسک وجود دارد. هر چه قابلیت پیش بینی پیشامدهای آینده کمتر باشد، ریسک بزرگ تر است. بنابراین، از آن جایی که هیچ کس به درستی قادر به پیش بینی آینده نیست، هر کسی بر حسب ضرورت دانش مدیریت ریسک را خواهان است و نیز تأثیر ریسک و مدیریت ریسک در سازمان ها به ویژه در سیستم های فناوری اطلاعات اجتناب

ناپذیر است، عنوان این پروژه «بررسی و مطالعه ی نقش مدیریت ریسک در سیستم های فناوری اطلاعات» انتخاب شده است.

۱-۳- هدف های پژوهش

هدف های کلی:

۱- بررسی نقش مدیریت ریسک در سیستم های فناوری اطلاعات.

۲- شناسایی استراتژی ها و ابزارهای مناسب مدیریت ریسک در کاهش، حذف و انتقال ریسک های زیان آور و چگونگی استفاده از آن ها.

هدف های فرعی:

۱- افزایش سودآوری و کاهش هزینه های عملیاتی و سربار

۲- افزایش سهم بازار

۳- افزایش توان رقابتی

۴- افزایش بهره وری سرمایه ی انسانی

۵- حفظ و ارتقای امنیت اطلاعات فروشگاه پویان کامپیوتر و مشتریان

۱-٤- پرسش های پژوهش

۱- نقش مدیریت ریسک در سیستم های فناوری اطلاعات چیست؟

۲- استراتژی ها و ابزارهای مناسب مدیریت ریسک در کاهش، حذف و انتقال ریسک های زیان آور چه مواردی هستند و چگونه می توان از آن ها در شرایط مختلف زمانی و مکانی استفاده کرد؟

۱-۵- قلمرو تحقیق

قلمرو زمانی: سال ۱۳۸۷

قلمرو مکانی: فروشگاه پویان کامپیوتر

قلمرو موضوعی: بررسی و مطالعه ی نقش مدیریت ریسک در سیستم های فناوری اطلاعات

۱-٦- روش تحقیق

در این تحقیق از روش های جستجو در اینترنت و منابع کتابخانه ای برای ادبیات تحقیق استفاده شده است. در بخش گردآوری اطلاعات تحقیق از روش توصیفی با استفاده از نرم افزار Expo-Se و ابزارهای مصاحبه و مشاهده و مطالعات اسناد و مدارک فروشگاه استفاده شده است.

۱-۷- محدودیت های تحقیق

به طور کلی هر تحقیق با محدودیت هایی مواجه است که تا حدی اهداف و رسیدن به نتایج دقیق و کامل را تحت تأثیر قرار می دهد. محدودیت های این تحقیق عبارتند از: کمبود اطلاعات در دسترس، فقدان الگوهای مناسب در زمینه تحقیق و جدید بودن عنوان تحقیق.

۱-۸- تعریف واژه های کلیدی

۱- ریسک[1]: عبارت است از توزیع از احتمال وقوع یک واقعه و پیامدهای آن (آذر، ۱۳۸۵).

۲- مدیریت ریسک فناوری اطلاعات[2]: مدیریت ریسک فرآیندی است که به مدیران فناوری اطلاعات اجازه می دهد تا هزینه های اقتصادی و عملیاتی سنجش های احتمالات خطر را متعادل کرده و با پشتیبانی از سیستم های فناوری اطلاعات و داده هایی که مأموریت های سازمان را پشتیبانی می کنند، از قابلیت های مأموریت بهره مند شوند (مؤسسه ی ملی استانداردها و فناوری).

۳- فناوری[3]: فناوری مجموعه‌ای از فرایندها، روش‌ها، فنون، ابزار، تجهیزات، ماشین‌آلات و مهارت‌هایی است که توسط آن ها کالایی ساخته شده یا خدمتی ارایه می شود (فتحیان و مهدوی نور، ۱۳۸۶).

٤- فناوری اطلاعات[4]: به مطالعه، طراحی، توسعه، پیاده سازی، پشتیبانی یا مدیریت سیستم های اطلاعاتی مبتنی بر رایانه، خصوصاً برنامه های نرم افزاری و سخت افزار رایانه می پردازد (انجمن فناوری اطلاعات آمریکا).

۵- اطلاعات[5]: داده های پردازش شده را اطلاعات می گویند (مک لوید، ۱۹۹۷).

---

[1] - Risk
[2] - Risk Management
[3] - Technology
[4] - Information Technology
[5] - Information

٦- امنیت اطلاعات[6]**:** امنیت اطلاعات یعنی حفاظت اطلاعات و سیستم‌های اطلاعاتی از فعالیت‌های غیرمجاز (فتحیان و مهدوی نور، ۱۳۸۶).

۷- مدیریت خطر یا مدیریت ریسک: کاربرد سیستماتیک سیاست‌های مدیریتی، رویه‌ها و فرایندهای مربوط به فعالیت‌های تحلیل، ارزیابی و کنترل ریسک می‌باشد. مدیریت ریسک عبارت از فرایند مستندسازی تصمیمات نهایی اتخاذ شده و شناسایی و به‌کارگیری معیارهایی است که می‌توان از آن‌ها جهت رساندن ریسک تا سطحی قابل قبول استفاده کرد (فرهنگستان زبان و ادب فارسی).

۱-۹- جمع بندی و مباحث فصول آینده

در این فصل به کلیات تحقیق اشاره شد. در فصل دوم به ادبیات پژوهش، در فصل سوم به ارایه روش پژوهش، در فصل چهارم به تجزیه و تحلیل اطلاعات و در فصل پنجم به نتیجه گیری و پیشنهادها اشاره خواهد شد.

[6] - Securyفناوری اطلاعات

فصل دوم: ادبیات پژوهش

۲-۱- مقدمه

موفقیت هر شرکتی از طریق بهره برداری از فرصت ها در کسب مزیت رقابتی به دست می آید و فناوری های اطلاعاتی برای استفاده از مزیت های این فرصت ها تنظیم و اجرا می شوند تا چیز جدیدی ساخته شود و یا تسهیلات موجود تغییر داده شوند. عنصر کلیدی تغییر، تصمیم گیری است که به صورت آرمانی چنین تصمیم هایی باید بر اساس اطلاعات کاملی با درجه‌ی قطعیت خروجی ها، شکل گیرند. با این وجود در دنیای واقعی، اغلب تصمیم ها بر اساس اطلاعات ناقص همراه با سطحی از عدم قطعیت راجع به خروجی ها اتخاذ می شود که این عدم قطعیت منجر به ریسک می شود. بنابراین، ریسک بخش ذاتی از هر سازمانی است. می توان مشاهده کرد که عدم قطعیت و فرصت بسیار نزدیک به هم هستند، وقتی ریسکی اتفاق می افتد می تواند تبدیل به فرصت شود و برعکس، فرصتی که همراه با ریسک است می تواند سازمان را از مسیر اصلی خود خارج سازد.

۲-۲- مدیریت ریسک سیستم های فناوری اطلاعات

ریسک را می توان توزیعی از احتمال وقوع یک حادثه و پیامدهای آن دانست. مدیریت ریسک یک بخش اصلی از مدیریت استراتژیک در هر سازمان و فرآیندی است که از طریق آن سازمان ها به صورت نظام مند با خطراتی که مربوط به فعالیت سازمان است روبه‌رو می شوند تا بتوانند منابعی پایدار بر فعالیت خود کسب کنند. نقطه تمرکز یک مدیریت ریسک کارآمد عبارت است از شناسایی و برطرف کردن این خطرها.

مدیریت ریسک باید فرآیند مستمر رو به رشد باشد و کلیه برنامه ها و استراتژی های سازمان و نحوه اجرای آن ها را مورد توجه قرار دهد. این مدیریت باید به صورت هدفمند برای کلیه خدماتی که در خصوص فعالیت های گذشته سازمان در آینده ظاهر می شود پاسخ متقاعد کننده داشته باشد.

مدیریت ریسک فرآیند شناسایی، ارزیابی و کنترل ریسک های اتفاقی بالقوه ای است که مشخصاً پیشامدهای ممکن آن خسارت یا عدم تغییر در وضع می باشد یا یک بخش استراتژیک در هر سازمان و فرآیندی است که از طریق آن سازمان ها به صورت نظام مند با خطرهایی که مربوط به فعالیت خود است روبه‌رو می شوند تا بتوانند منافعی پایدار در فعالیت خود کسب کنند. نقطه تمرکز، مدیریت ریسک یک شرکت را قادر می کند تا به نحو بهتری ریسک های متداول خود را اداره کند (راعی و سعیدی، ۱۳۸۳).

مدیریت ریسک سیستم های فناوری اطلاعات فرآیندی است که به مدیران فناوری اطلاعات اجازه می دهد تا هزینه های اقتصادی و عملیاتی سنجش های احتمالات خطر را متعادل کرده و با حمایت از سیستم

های فناوری اطلاعات و داده هایی که مأموریت های سازمان را پشتیبانی می کنند، از قابلیت های مأموریت بهره مند شوند. این فرآیند، مختص محیط فناوری اطلاعات نمی باشد، در واقع تصمیم گیری را در تمامی زمینه های زندگی روزمره وارد می کند (مؤسسه ی ملی استانداردها و فناوری).

۲-۳- عملیات کنترل ریسک

عملیات کنترل ریسک عبارت است از برنامه و اجرای مدیریت ریسک که در واقع آن را با استفاده از قابلیت های سازمانی و پایین ترین خرابی و هزینه، اجرایی می کند. کند (مؤسسه ی ملی استانداردها و فناوری)

همچنین، فرآیند پیشنهاد کنترل دربرگیرنده گزینش از میان ترکیبی کنترل های عملیاتی، مدیریتی و فنی برای بهبود وضع امنیتی سازمان است. کند (مؤسسه ی ملی استانداردها و فناوری)

کنترل به انواع مختلفی تقسیم می شود که شامل (مؤسسه ی ملی استانداردها و فناوری):

الف- کنترل های امنیت فنی

کنترل های امنیت فنی برای کاهش ریسک را می توان برای حمایت در برابر گونه های مشخص تهدیدات پیکربندی کرد. این کنترل ها از سنجش های ساده تا پیچیده گسترده بوده و معمولاً معماری های سیستم، نظام های مهندسی و بسته های امنیتی با ترکیبی از سخت افزار، نرم افزار و میان افزار را شامل می شود. تمامی این سنجش ها باید برای تأمین اطلاعات و داده های حساس و بحرانی، و وظایف سیستم فناوری اطلاعات در کنار یکدیگر به کار گرفته شوند. کنترل های فنی را می توان بر اساس هدف اولیه، به دسته های عمده زیر تقسیم بندی کرد:

- پشتیبانی.
- پیشگیرانه.
- آشکارسازی و ترمیم یک رخنه امنیتی.

ب- کنترل های فنی پشتیبانی

به طور طبیعی، کنترل های پشتیبانی فراگیر و با بسیاری دیگر از کنترل ها در ارتباط است. کنترل های پشتیبانی عبارتند از:

- شناسایی تمام کاربران، فرآیندها و منابع اطلاعاتی.

- مدیریت کلید پنهانی: کلیدهای پنهانی باید به هنگام پیاده سازی وظایف پنهان سازی در دیگر کنترل ها، با اطمینان مدیریت شوند. مدیریت کلید پنهانی دربرگیرنده تولید، توزیع، ذخیره و نگهداری کلید است.
- مدیریت امنیت: ویژگی های امنیتی یک سیستم فناوری اطلاعات باید در مواجهه با نیازهای نصب خاص و مورد نظر قرار دادن تحول های محیط عملیاتی، پیکربندی شوند. امنیت سیستم را می توان در امنیت سیستم عامل یا برنامه کاربردی ایجاد کرد. فرآورده های امنیتی اضافی و سفارشی در دسترس است.
- پشتیبانی های سیستم شامل استفاده مجدد از هدف، نیاز به آگاهی، جداسازی فرآیند، پیمانه ای کردن، لایه بندی و حداقل سازی آنچه مورد نیاز است.

پ- کنترل های فنی پیشگیرانه

این کنترل ها می توانند به تلاش در خط مشی های امنیتی محدود شوند، شامل:

- تصدیق: کنترل تصدیق، روشی را برای بررسی هویت یک موضوع ارایه کرده تا اعتبار هویت ادعا شده را تضمین کند. ساز و کارهای تصدیق عبارتند از: شناسه و رمز عبور، و پدیداری فناوری های تصدیق.
- اجازه: کنترل مجوز امکان مدیریت ویژگی و اقدام های مجاز آتی یک سیستم مشخص را فراهم می کند.
- الزام کنترل دسترسی: صحت داده ها و اعتمادپذیری در کنترل های دسترسی الزامی اند. زمانی که فاعل متقاضی دسترسی برای دسترسی به فرآیندهای خاصی احراز می شود، لازم است تا خط مشی امنیتی تعریف شده ای الزام شود. این کنترل های مبتنی بر خط مشی از طریق ساز و کارهای کنترل دسترسی توزیع شده در سیستم، الزام شده اند. اثربخشی و توان کنترل دسترسی به درستی تصمیم های کنترل دسترسی و شدت الزام کنترل دسترسی وابسته است.
- غیر قابل انکار: پاسخ گویی سیستم به توانایی تضمین عدم توانایی فرستنده در رد ارسال اطلاعات و عدم توانایی گیرنده در رد دریافت آن وابسته است. این صفت در هر دو نوع پیشگیرانه و کاشفانه توسعه یافته است ولی از آن جایی که ساز و کارهای پیاده سازی شده مانع رد موفق یک فعل می شوند، در این راهنما، در دسته پیشگیرانه جای گرفته است. در نتیجه، این کنترل نوعاً در نقطه ارسال یا دریافت استفاده می شود.

- ارتباط پشتیبانی شده: در یک سیستم توزیع شده، توانایی نیل به اهداف امنیتی به شدت به صحت ارتباط وابسته است. ارتباطات پشتیبانی شده ضامن صحت، دسترسی پذیری و اعتماد پذیری اطلاعات حساس و بحرانی بوده در حالی که این گذرا است. ارتباطات پشتیبانی شده از روش های رمزگذاری داده ها و توسعه فناوری های پنهان سازی برای حداقل کردن تهدیدهای شبکه مانند پاسخ، تفسیر، کنکاش بسته، استراق سمع یا ضبط مکالمه ها استفاده می کند.
- اختفای تراکنش: هر دو سیستم بخش دولتی و خصوصی نیازمند حفظ حریم افراد می باشند. کنترل های اختفای تراکنش مانع از دست رفتن محرمانگی با توجه به تراکنش انجام شده توسط یک فرد، می شوند.

ت- کنترل های فنی آشکارسازی و ترمیم

کنترل های آشکارسازی نسبت به تجاوزات خط مشی امنیتی هشدار داده و شامل کنترل هایی مانند بررسی اثر، روش های کشف نفوذ و فهرست مقابله ای است. کنترل های بازیابی را می توان در بازیابی منابع محاسباتی از دست رفته استفاده کرد. آن ها به عنوان مکمل سنجش های فنی پیشگیرانه و پشتیبانی موردنیاز می باشند، زیرا هیچ یک از سنجش های زمینه های دیگر کامل نیست. کنترل های آشکارسازی و ترمیم شامل:

- بازبینی: بازبینی رخدادهای مربوط به امنیت و نظارت و پیگیری ناهنجاری های سیستم، عنصرهای کلیدی آشکارسازی و ترمیم شکاف های امنیتی است.
- آشکارسازی محدود سازی تهاجم: آشکارسازی شکاف های امنیتی به طوری که پاسخ به موقع انجام شود. در صورتی که پاسخ مؤثری داده نشود، از آشکارسازی شکاف امنیتی کمتر استفاده خواهد شد. آشکارسازی تهاجم و کنترل محدود سازی این دو قابلیت را فراهم می آورند.
- برهان تمامیت: کنترل برهان تمامیت صحت و بی نظمی های سیستم را تحلیل کرده و تهدیدهای آشکار و بالقوه را شناسایی می کند. این کنترل مانع تجاوز به خط مشی امنیتی نشده ولی تجاوزها را آشکار و به تعیین اقدام اصلاحی کمک می کند.
- بازیابی وضعیت امن: این سرویس سیستم را قادر می کند تا پس از بروز شکاف امنیتی، به وضعیت امن بازگردد.

- آشکارسازی و ریشه کنی ویروس: آشکارسازی و ریشه کنی ویروس نرم افزار نصب شده روی سرورها و ایستگاه های کاری کاربران، برای تضمین صحت داده ها و سیستم، ویروس های نرم افزاری را آشکار، شناسایی و حذف می کند.

ث- کنترل های امنیت مدیریت

کنترل های امنیت مدیریت در الحاق با کنترل های عملیاتی و فنی، برای مدیریت و کاهش ریسک زیان و پشتیبانی از مأموریت یک سازمان، پیاده سازی شده اند. کنترل های مدیریت روی تصریح خط مشی پشتیبانی اطلاعات، رهنمودها و استانداردهایی متمرکز هستند که در طی رویه های عملیاتی برای تکمیل اهداف و مأموریت های سازمان انجام شده اند.

ج- کنترل های پیشگیرانه امنیت مدیریت

این کنترل ها شامل:

- انتساب مسئولیت امنیت برای تضمین ارایه امنیت کافی برای سیستم های فناوری اطلاعات مأموریت بحرانی
- توسعه و نگهداری برنامه های امنیتی سیستم برای مستندسازی کنترل های جاری و آدرس دهی کنترل های برنامه ریزی شده برای سیستم فناوری اطلاعات برای پشتیبانی مأموریت سازمان
- پیاده سازی کنترل های امنیتی پرسنل مانند جداسازی وظایف، حداقل امتیازها و خاتمه و ثبت دسترسی رایانه کاربر
- هدایت آگاهی امنیتی و آموزش فنی برای تضمین آگاهی کاربران نهایی و کاربران سیستم از قوانین رفتار و مسئولیت های خود در پشتیبانی از مأموریت سازمان.

چ- کنترل های امنیت مدیریت آشکارسازی

کنترل های مدیریت آشکارسازی شامل:

- پیاده سازی کنترل های امنیت کارکنان
- هدایت بازنگری دوره ای کنترل های امنیت برای تضمین اثربخشی کنترل ها
- انجام بررسی های دوره ای سیستم
- هدایت مدیریت ریسک مداوم برای ارزیابی و کاهش ریسک
- احراز سیستم های فناوری اطلاعات برای آدرس دهی و پذیرش ریسک باقیمانده

ح- کنترل های امنیت مدیریت بازیابی

این کنترل ها شامل:

- ایجاد تداوم پشتیبانی و توسعه، تست و حفظ تداوم برنامه عملیات ها برای ایجاد از سرگیری کار و تضمین تداوم عملیات در طی بروز حوادث
- ایجاد قابلیت واکنش نسبت به حوادث برای آماده سازی تشخیص، گزارش و واکنش نسبت به حادثه و بازگشت سیستم فناوری اطلاعات به وضعیت عملیاتی

خ- کنترل های امنیت عملیاتی

استانداردهای امنیت یک سازمان باید مجموعه ای از کنترل ها و رهنمودها را برای تضمین الزام و پیاده سازی نظارت مناسب رویه های امنیتی بر کاربرد منابع و دارایی های فناوری اطلاعات سازمان بر طبق مأموریت و اهداف سازمان، ایجاد کند. مدیریت، نقشی اساسی را در سرپرستی، پیاده سازی خط مشی و تضمین ایجاد کنترل های عملیاتی مناسب، ایفا می کند.

کنترل عملیاتی که منطبق بر مجموعه ای پایه از الزام ها و شیوه های صنعتی پیاده سازی شده اند، در تصحیح نواقص عملیاتی مورد استفاده منابع- تهدید بالقوه، کاربرد دارند. برای تضمین سازگاری و یکپارچگی عملیات امنیتی، باید روش ها و رویه های گام به گام پیاده سازی کنترل های عملیاتی به روشنی تعریف، مستند و نگهداری شوند.

د- کنترل های امنیتی پیشگیرانه

این کنترل ها عبارتند از:

- کنترل مصرف و دسترسی رسانه داده ها
- محدودسازی توزیع داده بیرونی
- امکان محاسبه امنیت
- سیم کشی امن محل نگهداری هاب ها و کابل ها
- ارایه قابلیت پشتیبان گیری
- ایجاد امنیت و رویه های ذخیره خارج از محل
- پشتیبانی از لپ تاپ ها، رایانه های شخصی ایستگاه های کاری
- پشتیبانی از دارایی های فناوری اطلاعات در برابر خسارت
- ایجاد منبع توان اضطراری

- کنترل رطوبت و دمای وسیله محاسباتی

ذ- کنترل های عملیاتی آشکارسازی

کنترل های آشکارسازی شامل:

- ایجاد امنیت فیزیکی
- تضمین امنیت محیطی

۲-٤- ریسک باقیمانده

سازمان ها قادر هستند تا گستره کاهش ریسک حاصل از کنترل جدید یا ارتقا یافته را برحسب اثر یا احتمال تهدید تقلیل یافته تحلیل کنند، دو معیاری که سطح بزرگی ریسک را برای مأموریت سازمان تعیین می کنند.

هدف فرآیند کنترل پردازش ریسک، شناسایی ریسک هایی است که کاملاً آدرس دهی نشده اند و تعیین نیاز کنترل های اضافی برای تخفیف ریسک های شناسایی شده در سیستم فناوری اطلاعات است. هر ریسک باقیمانده ای پذیرفته و عملیات سیستم فناوری اطلاعات جدید تأیید یا پردازش سیستم فناوری اطلاعات جاری ادامه پیدا می کند. اگر ریسک باقیمانده تا سطح قابل قبولی کاهش پیدا نکند ، چرخه ی مدیریت ریسک باید برای شناسایی راه جدیدی برای تقلیل ریسک باقیمانده به سطحی قابل قبول، تکرار شود (مؤسسه ی ملی استانداردها و فناوری).

۲-۵- تجزیه و تحلیل هزینه- درآمد

برای تخصیص و پیاده سازی کنترل های هزینه- سود پس از شناسایی تمام کنترل های احتمالی و ارزیابی امکان پذیری و اثربخشی آن ها، باید یک تجزیه و تحلیل هزینه- درآمد را برای تعیین کنترل های لازم و مناسب با شرایط، برای هر کنترل پیشنهادی هدایت کرد.

تجزیه و تحلیل هزینه- درآمد می تواند کمی یا کیفی باشد. هدف آن شرح چگونگی تعدیل هزینه های پیاده سازی کنترل ها به کمک کاهش سطح ریسک است.

تجزیه و تحلیل هزینه- درآمد برای کنترل های پیشنهادی جدید یا پیشرفته، موارد زیر را شامل می شود:

- تعیین اثر پیاده سازی کنترل های جدید یا پیشرفته
- تعیین اثر عدم پیاده سازی کنترل های جدید یا پیشرفته

- برآورد هزینه های پیاده سازی که می تواند موارد زیر را شامل شود:

- خرید نرم افزار و سخت افزار
- کاهش اثربخشی عملیاتی در صورت کاهش وظیفه ای بودن یا عملکرد به ازای افزایش امنیت
- هزینه پیاده سازی رویه ها و خط مشی های اضافی
- هزینه به کارگیری کارکنان اضافی برای انجام خط مشی ها، رویه ها و یا خدمات پیشنهادی
- هزینه های آموزش
- هزینه های نگهداری

- ارزیابی منافع و هزینه های پیاده سازی در مقابل حساسیت سیستم و داده ها در جهت تعیین ارزش پیاده سازی کنترل های جدید برای سازمان، با توجه به هزینه ها و اثر مشخص.

سازمان نیازمند ارزیابی منافع کنترل ها بر حسب نگهداری طرح مأموریت قابل قبول برای سازمان خواهد بود. از آن جا که پیاده سازی کنترل موردنظر هزینه ای دارد، عدم پیاده سازی آن نیز هزینه بر خواهد بود. با ارتباط برقرار کردن نتیجه عدم پیاده سازی کنترل و مأموریت سازمان، می توان امکان پذیری پیاده سازی آینده را تعیین کرد.

۲-٦- تخمین یا برآورد ریسک

تخمین ریسک می تواند برحسب احتمال رخداد و پی آمد آن کمی یا نیمه کمی و حتی کیفی باشد. مثلاً هر کدام از پیامدهای تهدیدآمیز (ریسک های نهایی) و فرصت ها (ریسک های ظاهری) ممکن است بالا، متوسط یا پایین باشند. احتمال نیز ممکن است بالا، متوسط و یا پایین باشد ولی در هر صورت نیاز به تعارفی متفاوت در زمینه تهدیدها و فرصت احساس می شود.

در تخمین یا برآورد ریسک می توان از فرمول زیر که توسط شرکت IBM انتشار یافته است، استفاده کرد:

$$R = P(h) \times P(a) \times L$$

P (h): احتمال کلی خطر اتفاق افتاده، P (a): احتمال کلی خطری که با یک تصادف درگیر خواهد شد و L بدترین حالت ممکن که توسط تصادف قابلیت ها از دست رفته باشند.

۲-۷- نتیجه گیری

شکی نیست که سیمای پروژه ها آرایش عظیمی از عدم اطمینان هایی است که قابلیت زیادی برای اثرگذاری بر اهداف نهایی آن ها دارند. همچنین آشکار است که برخی از عدم اطمینان ها ممکن است در صورت به وقوع پیوستن سودآور باشند. همان طور که در بسیاری از موارد می تواند منشأ آسیب رساندن به سازمان باشند. کاربران مدیریت ریسک به طور فزاینده ای این مطلب را پذیرفته اند که تعریف ریسک به عنوان «عدم اطمینانی که می تواند بر اهداف اثر بگذارد» شامل فرصت ها و تهدیدها می شود و آن ها باید توسط مدیران ریسک به طور پویا مدیریت شوند.

فصل سوم: روش شناسی

۳-۱- مقدمه

روش شناسی وسیله شناخت هر علم است. روش شناسی در مفهوم مطلق خود به روش هایی گفته می شود که برای رسیدن به شناخت علمی از آن ها استفاده می شود و روش شناسی هر علم نیز روش های مناسب و پذیرفته آن علم برای شناخت هنجارها و قواعد آن است (ضیائی بیگدلی، ۱۳۸۴).

یکی از اصلی ترین بخش های هر کار پژوهشی را جمع آوری اطلاعات تشکیل می دهد. چنان چه این کار به شکل منظم و صحیح انجام شود، کار تجزیه و تحلیل و نتیجه گیری از داده ها با سرعت و دقت خوبی انجام خواهد شد.

۳-۲- روش های گردآوری اطلاعات

در این تحقیق از روش های کیفی کتابخانه ای و میدانی برای گردآوری اطلاعات استفاده شده است.

۳-۳- ابزارهای گردآوری اطلاعات

ابزارهای مورد استفاده برای گردآوری اطلاعات عبارتند از: مشاهده، مصاحبه، بررسی اسناد و مدارک سازمانی، مقالات و کتاب های مرتبط با عنوان پژوهش.

۳-٤- روش تجزیه و تحلیل اطلاعات

اقدام پژوهی

فصل چهارم: تجزیه و تحلیل داده ها

٤-١- مقدمه

در این فصل برای تجزیه و تحلیل اطلاعات فروشگاه پویان کامپیوتر به بررسی موارد زیر بسنده خواهد شد:

۱) ارزیابی ریسک
۲) اعمال، امنیت و مدیریت ریسک
۳) برنامه گزارش/ دوره استقلال
۴) مرور مجدد حوادث و ادامه کسب و کار
۵) نظام و قانون های Gramm- Leach- Bliley Act/ FDIC-12CFR
۶) فرهنگ و پشتیبانی سازمانی
۷) سیاست مدیریت ریسک
۸) اهداف سازمانی
۹) شناسایی ریسک
۱۰) تجزیه و تحلیل ها، ارزیابی و رفتار ریسک
۱۱) نظارت و دوره کردن ریسک
۱۲) مدیریت ریسک اثربخش

٤-٢- بخش ۱- ارزیابی ریسک

هدف فروشگاه پویان کامپیوتر برای ارزیابی ریسک شامل تجزیه و تحلیل های تهدیدهای داخلی و خارجی مشتریان و اطلاعات فروشنده، فرآیندهای نگهداری دارایی ها، سیاست های امنیت اطلاعات و فرآیندها و استراتژی های مشخص شده‌ی مستند کاهش ریسک است، برنامه رسمی ارزیابی ریسک حداقل سالیانه توسط هیئت مدیره تأیید می شود و همچنین برای بازخوانی و مرور و تأیید کردن ارزیابی ریسک توسط هیئت مدیره ماهانه انجام می شود.

٤-٣- بخش۲- اعمال، امنیت و مدیریت ریسک

از آن جا که همواره امنیت در فرآیند برنامه ریزی استراتژیک گسترش پیدا می کند و سیاست ها یا فرآیندهای درستی برای در اختیار داشتن اطلاعات وجود دارند، این فروشگاه برنامه امنیت اطلاعات خود را

در جهت مدیریت کردن ریسک ها بر پایه اعمال سیاست ها، فرآیندها و راهنمایی هایی برای امنیت، نگهداری و نظارت سیستم ها و پایگاه داده های مستقر کرده است. برای نیل به ا ین هدف، کارکنان این فروشگاه از برنامه های ضد ویروس، ضد جاسوسی و رمزنگاری برای برنامه حسابداری و سایر اطلاعات اساسی فروشگاه در برابر مورد ناآشنا و تهدیدهای دیجیتالی استفاده می کنند.

٤-٤- بخش۳- برنامه گزارش / دوره استقلال

این فروشگاه برنامه دوره ای مستقل از گزارش های فناوری اطلاعات را در اختیار دارد و این گزارش ها شامل مقایسه پیکربندی های سیستم واقعی برای استانداردهای پیکربندی مستند و اساسی، فرآیند ارزیابی ریسک و ارزیابی کاربران و حقوق ورودی کاربران سیستم هستند و همچنین در این گزارش ها تا اندازه کمی به تضادهای شناخته شده و تراکم فعالیت ها اشاره می شود.

٤-٥- بخش٤- مرور مجدد حوادث و ادامه کسب و کار

فروشگاه پویان کامپیوتر برنامه مرور مجدد حوادث و ادامه کسب و کار خدو را بر اساس برنامه ریزی بر روی تجزیه و تحلیل کسب و کار دائمی و عادی خود انجام می دهد و مرور مجدد حوادث و ادامه کسب و کار آن شامل ارزیابی ریسک است. بنابراین، فروشگاه می تواند با استناد به این تجزیه و تحلیل ها، برنامه ریزی ها و ارزیابی ریسک به فعالیت خود ادامه دهد.

٤-٦- بخش ٥- نظام و قانون های Gramm- Leach- Bliley Act/ FDIC-12CFR

مدیریت یک دسته از برنامه امنیت اطلاعات را با استفاده از استانداردهای امنیت اطلاعات گسترش می دهد و گزارش های کاملی از استانداردها به صورت دوره ای انجام می شوند و به طور رسمی به هیئت مدیره گزارش می شوند.

٤-٧- بخش ٦- فرهنگ و پشتیبانی سازمانی

این فروشگاه ارتباط بسته ای را بین اهداف استراتژیک و مدیریت ریسک را توسعه می دهد. تلاش مدیریت ریسک برای افزایش سود کارکنان و مدیران فروشگاه می باشد. مسئول پشتیبانی برای مدیریت ریسک بر عهده مدیر فروشگاه و کارکنان است. مدیر ریسک همواره یک نقش تسهیلاتی برای افزایش

آگاهی مدیران و کارکنان از مزایای مدیریت ریسک، پیشرفت قابل قبول فنون مدیریت ریسک، توسعه سیاست ها و فرآیندهای مدیریت ریسک را ایفا می کند.

٤-٨- بخش ۷- سیاست مدیریت ریسک

مدیریت ریسک، سیاست های مدیریتی خود را در جلسات ماهیانه با مدیرعامل فروشگاه تأیید یا رد می کند. سیاست مدیریت ریسک فروشگاه با استفاده از دوره های آموزشی و نظام مدیریتی اعلام می شود و مراحل پیروی از توسعه سیاست مدیریت ریسک توسط تمامی مدیران و کارکنان گزارش می شود.

٤-٩- بخش ۸- اهداف سازمانی

اهداف سازمانی فروشگاه پویان کامپیوتر شامل یک بیانیه مستند، قابل فهم و مرتبط با شرح وظایف مدیران و کارکنان است.

برای دستیابی به سود و رشد فروشگاه، مدیران ریسک و مالی تحلیل های سناریو را در برنامه خود قرار می دهند تا فعالیت هایی که ریسک دارند بودجه بندی شوند.

٤-١٠- بخش ۹- شناسایی ریسک

مدیریت ریسک، ریسک های مرتبط با اهداف فروشگاه را شناسایی می کند. برای انجام شناسایی ریسک ها که برای توسعه فروشگاه لازم هستند موارد راهبردی، عملیاتی، ریسک های مورد اعتماد عمومی، ریسک های فناوری، انسانی و امنیتی رعایت می شوند. فنونی که برای شناسایی ریسک در فروشگاه پویان کامپیوتر استفاده می شوند عبارتند از:

۱) سناریوسازی
۲) مصاحبه
۳) پژوهش ها
۴) تجربه های گذشته سازمانی
۵) تجزیه و تحلیل های فرآیندی

٤-١١- بخش١٠- تجزیه و تحلیل ها، ارزیابی و رفتار ریسک

در فروشگاه پویان کامپیوتر، ریسک ها بر اساس نتایج، ضررهای مالی و دستیابی به اهداف از طریق روش های تجزیه و تحلیل های کیفی ارزیابی می شوند. پاسخگویی مدیریت ریسک به ریسک های تجزیه و تحلیل شده شامل ارزیابی هزینه ها و سودهای ناشی از انتقال و دوره ریسک ها و انتخاب مواردی که به مدیریت فعال نیاز دارند و دوره رفتارهای ریسک که بر منابع و محدودیت ها تأثیر می گذارند، است. مدیریت ریسک از گزینه رفتار ریسک، برای نرخ دادن یا قبول کردن ریسک، خودداری از پذیرش ریسک، کاهش ریسک و انتقال ریسک استفاده می کند.

٤-١٢- بخش١١- نظارت و دوره کردن ریسک

مدیریت ماهیانه ریسک های مشاهده شده، رفتارهای ریسک اثربخش یا کاربردی و فرصت ها را دوره و نظارت می کند و گزارش خود را برای نیل به مدیریت ریسک اثربخش به همکاران اعلام می کند.

٤-١٣- بخش ١٢- مدیریت ریسک اثربخش

عواملی که باعث اثربخشی مدیریت ریسک در فروشگاه پویان کامپیوتر شده اند عبارتند از:

۱) ایجاد ارتباط بین اهداف و ریسک ها
۲) تدوین درجه ریسک پذیری فروشگاه
۳) اندازه گیری رفتار ریسک
۴) ایجاد استاندارد و معیاری برای ارزیابی ریسک
۵) شناسایی، ضبط، تجزیه و تحلیل و دوره کردن ریسک ها
۶) استفاده از نرم افزار Expo- se برای تجزیه و تحلیل کردن ریسک ها
۷) ارایه گزارش های منظم به مدیران و کارکنان برای رویارویی با ریسک ها توسط مدیر ریسک

فصل پنجم: نتیجه گیری و پیشنهادها

۵-۱- نتیجه گیری

خدمات و فعالیت های سازمان های هوشمند برای استفاده تجهیزات در ریسک بلندمدت به صورت مرحله ای و فرآیندی است. با این منظور که ابتدا نحوه ی کاربرد تجهیزات و استراتژی ها به مدیران و کارکنان آموزش داده شده و سپس آن تجهیزاتی که در ارتباط با موضوع ریسک هستند گردآوری شده و استفاده می شوند. همچنین، بخش های مختلف آن ها در کاهش یا حفظ هزینه های مالی و افزایش منافع مادی برای سازگاری با یکدیگر و محیط اطراف خود موارد زیر را در نظر می گیرند:

- شناخت از وضعیت بازار، رقبا، محیط های اقتصادی، سیاسی و فناوری و همچنین نیازهای مشتریان
- کیفیت، مقدار، قیمت، کمیت و منبع مناسب کالاها و خدمات

مدیران سازمان های هوشمند با استفاده از موارد زیر ریسک های موجود را برای دستیابی به اهداف خود و شرکت مدیریت می کنند:

- تحلیل کیفی ریسک با استفاده از ابزارهای برگزاری جلسه های خبرگان و سناریوسازی
- برنامه ریزی واکنش ریسک با استفاده از برنامه Expo- se و استراتژی های بیان شده در فصل ادبیات تحقیق
- تخمین یا برآورد ریسک با استفاده از فرمول منتشر شده توسط شرکت IBM
- مدیران ریسک با استناد به تجزیه و تحلیل هزینه- درآمد و تعدیل هزینه های پیاده سازی کنترل درآمدها و هزینه های شرکت ارزیابی می کند.

۵-۲- پیشنهادها

پیشنهاد می شود فروشگاه پویان کامپیوتر برای دستیابی به اهداف مدیریت ریسک به نکات زیر توجه کند:

۱- سطح نوآوری فروشگاه بالا باشد تا بتواند در بازار رقابت کند.

۲- استفاده از زبان صریح و قابل فهم برای ارایه ی بیانیه ها، اسناد و مدارک

۳-کار کردن نزدیک با مشتری

۴- تخمین و برآورد قوی از عملکردها و ریسک های فروشگاه

۵- برنامه ریزی و کنترل کافی و مناسب برای اجرای فرآیندها و عملیات کاهش ریسک سیستم های فناوری های اطلاعاتی

۶- از استراتژی های مناسب مدیریت ریسک به شکل اقتضایی برای سیستم های فناوری اطلاعات استفاده شود.

منابع:

آمار و احتمالات و کاربرد آن در مدیریت، عادل آذر و منصور مؤمنی، ۱۳۸۵، انتشارات سمت، جلد دوم.

فرهنگستان زبان و ادب فارسی.

مبانی مهندسی مالی و مدیریت ریسک، راعی و سعیدی، ۱۳۸۳، انتشارات سمت، چاپ دوم.

مبانی و مدیریت فناوری اطلاعات، محمد فتحیان، حاتم مهدوی نور، تهران، دانشگاه علم و صنعت، ۱۳۸۶، چاپ ششم

متدلوژی حقوق بین الملل. مجله پژوهش حقوق و سیاست، محمدرضا ضیائی بیگدلی، ۱۳۸۴، سال ۷، ش. ۱۵ و ۱۶.

http://www.idsco.ir/information_security_assey

www.IBM.com

Risk Management Guide for Information Technology Systems, G Stoneburner, Alice Y. Goguen, Alexis Feringa, 2002, Available at:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf

ضمیمه - معرفی فروشگاه پویان کامپیوتر

فروشگاه پویان کامپیوتر در سال ۱۳۷۸ توسط آقای مهندس فرهاد فردوسی (کارشناس مهندسی سخت افزار) با عضویت در اتحادیه صنفی کامپیوتر اصفهان تأسیس شد.

اهداف این بنگاه اقصادی عبارتند از:

۱- ایجاد رضایت مشتریان

۲- بهبود کیفیت، اثربخشی و کارآیی کالاها و خدمات

۳- به روز رسانی مشتریان داخلی و خارجی

فعالیت های پویان کامپیوتر شامل:

۱- خرید و فروش محصولات فناوری اطلاعات

۲- طراحی، پیاده سازی و ارزیابی و نظارت بر پروژه های شبکه های رایانه ای

۳- پشتیبانی و مشاوره فناوری اطلاعات

Ministry of Science, Researches & Education

Sheikhbahaei University

The Bachelor Project of Business Management

Title:
Surveying and Studying of Role of Risk Management on Information Technology

Lecturer:
Mr. Masoud Nasr Esfahani

Researcher:
Arash Ahmadi Esfahani

2008