

مدیریت ریسک و ارزش در امنیت سایبری سازمانی

محمدامین صادقی^۱، حسین کارگر^۲، مهدی اکبری دهبیری^۳، علی مصلی نژاد^۴

^۱ باشگاه پژوهشگران جوان و نخبگان، واحد جهرم، دانشگاه آزاد اسلامی، جهرم، ایران

^۲ گروه مهندسی برق واحد جهرم، دانشگاه آزاد اسلامی، جهرم، ایران

^۳ گروه مهندسی برق واحد جهرم، دانشگاه آزاد اسلامی، جهرم، ایران

^۴ دپارتمان مهندسی فناوری اطلاعات، دانشگاه آزاد اسلامی، واحد الکترونیکی، تهران، ایران

چکیده

مدیریت ریسک را می‌توان فرآیندی برای حفظ دارایی‌ها، قدرت و امنیت دانست و مهندسی ارزش، مدیریت ارزش بخشی جدایی ناپذیر از مدیریت ریسک به حساب می‌آید. یکپارچه سازی مهندسی ارزش و مدیریت ریسک باعث ایجاد هم افزایی می‌شود؛ این هم افزایی وقتی در امنیت سایبری پیاده شود، می‌تواند بر امنیت سایبری تاثیر بگذارد. این مقاله ارزیابی ریسک امنیت سایبری مبتنی بر ارزش، درجه تاثیر و درجه سختی بررسی می‌کند. در این پژوهش با هدف کسب نظر خبرگان درباره ریسک های امنیت اطلاعات سازمانی پرسشنامه بین خبرگان توزیع شد، از میان عوامل امنیت اطلاعات ۵۵ ریسک امنیتی استخراج شد که سرانجام در قالب ۱۵ ریسک امنیتی مشخص شد. در این پرسشنامه، هر یک از خبرگان که تعداد آنها ۱۰ نفر بود نظر خود را درباره میزان ریسک تک تک عوامل برای امنیت اطلاعات در طیف پنج گانه لیکرت از طریق متغیرهای کلامی (خیلی کم، کم، متوسط، زیاد و خیلی زیاد) و با رویکردی مدیریت ارزش ابراز کردند. درجه تاثیر هزینه هر ریسک و سختی آن برای سازمان مشخص شد. در این مطالعه که مطالعه تطبیقی بین ریسک ها از نظر ارزش آن ها برای سازمان بود، یافته ها نشان داد عملکرد توأم مدیریت ریسک و مهندسی ارزش در امنیت، با افزایش امنیت همراه خواهد بود بوده است.

واژه‌های کلیدی: امنیت سایبر، ارزیابی ریسک امنیتی، مدیریت ریسک، ارزش

۱. مقدمه

مدیریت ریسک را می‌توان فرآیندی برای حفظ دارایی‌ها و قدرت کسب درآمد دانست و مهندسی ارزش، مدیریت ارزش بخشی جدایی ناپذیر از مدیریت ریسک به حساب می‌آید. یک پارچه سازی مهندسی ارزش و مدیریت ریسک باعث ایجاد هم افزایی می‌شود. موضوع امنیت اطلاعات در سازمان‌ها، استفاده از سیستم‌های امنیت اطلاعات را با چالش ریسک مواجه کرده است. چنانچه فرایند مدیریت ریسک در این سیستم‌ها به درستی انجام شود، می‌توان به اجرای موفق آن دست یافت (فنگ و همکاران، ۲۰۱۴).

به طور کلی مدیریت ریسک شامل سه گام اساسی شناسایی ریسک، ارزیابی ریسک و برنامه ریزی کاهش ریسک است. در شناسایی و تعیین میزان ریسک سیستم‌های اطلاعاتی، مشکلاتی مانند نبود داده‌های آماری، موجب می‌شود مقادیر نادرستی برای ریسک سیستم‌های اطلاعاتی، محاسبه شود. از این رو اغلب روش‌های ارزیابی ریسک برای سیستم‌های اطلاعاتی بر پایه معیارهای کیفی بنا شده‌اند نه معیارهای کمی. با این حال، ارزیابی کیفی ریسک برای شناسایی ریسک‌ها تا حدودی ذهنی است. (لو و چن، ۲۰۱۲).

موسسه ملی استاندارد و فناوری (NIST) مدیریت ریسک را به صورت "فرایند شناسایی ریسک، ارزیابی ریسک، و طی مراحل برای کاهش ریسک به سطحی قابل قبول" تعریف می‌کند (میراسکندری، ۲۰۱۰). NIST ارزیابی ریسک را به صورت فرایند شناسایی، تخمین و اولویت بندی ریسک‌های امنیت اطلاعات تعریف می‌کند که نیازمند تحلیل دقیقی از تهدیدها و اطلاعات آسیب پذیری برای تعیین میزانی است که در آن شرایط یا رویدادها می‌توانستند تأثیر معکوسی بر سازمان و احتمال اینکه چنین شرایط یا رویدادهایی رخ دهند، داشته باشند.

هدف مدیریت امنیت اطلاعات هر سازمان، حفظ سرمایه‌های سازمان (نرم افزاری، سخت افزاری، اطلاعاتی و ارتباطی و نیروی انسانی) در برابر هرگونه تهدید (دسترسی غیر مجاز به اطلاعات، خطرهای ناشی از محیط و سیستم و خطرهای ایجاد شده از سوی کاربران) است و برای دستیابی به این اهداف به برنامه منسجمی نیاز دارد. مدیریت سیستم امنیت اطلاعات راهکاری برای رسیدن به این اهداف است؟ (چین و همکاران، ۲۰۰۹).

بهره‌گیری مجزا از دو رویکرد مهندسی ارزش و مدیریت ریسک در پروژه‌ها پیشینه‌ای طولانی دارد. تلفیق اثر بخش آنها مورد توجه پژوهشگران به ویژه دالاس (۲۰۰۶) قرار گرفته است. در این مقاله کوشش می‌شود تا الگویی ساده تر و کاربردی با محوریت بهینه سازی شاخص ارزش ایده‌های برتر حاصل از کارگاه مهندسی ارزش همراه با مدیریت ریسک برای امنیت اطلاعات ارائه کند.

شاخص ارزش بهینه شده از ضرب نمودن عامل ریسک در شاخص ارزش معمول، حاصل می شود. این شاخص با شفاف سازی مزایا و معایب هر ایده، تصمیم گیری اثر بخش مدیریت ارشد را تسهیل می کند. در واقع، ریسک شرایط یا رخدادهای نامعلومی است که اگر اتفاق بیفتد اثر مثبت یا منفی بر حداقل یکی از اهداف پروژه دارد (حسینی و ذکایی آشتیانی، ۱۳۸۵). ارزش عبارت است از نسبت کارکرد به هزینه. ارزش می تواند از طریق بهبود کارکرد یا کاهش هزینه افزایش یابد. مطالعات ارزش، فرصت های مناسبی برای کاهش هزینه ی طول عمر، بهبود کیفیت کاهش زمان ساخت، افزایش طول عمر و گاه ترکیبی از این ها را در اختیار قرار می دهد.

تحت فشار قرار گرفتن مدیران در پذیرش و اعمال تغییرات پیشنهادی از یک سو و مسئولیت ایشان در قبال حوزه ی تحت اختیار خود به همراه ریسک و ابهام ذاتی گزینه های پیشنهادی از سوی دیگر، اغلب مدیران را در وضعیت دشواری قرار می دهد. از این رو بسیاری از مدیران به دلیل ابهام در مورد میزان ریسک گزینه های ارائه شده در مطالعات مهندسی ارزش، از پذیرش و انجام آن ها سر باز زده یا در طول مطالعات مقاومت می کنند. از اثرات این تصورات می توان به انتخاب گزینه های کم خطر و اغلب کم خطر و اغلب کم ارزش تر، رد گزینه های خلاقانه، عدم تناسب ریسک در تصمیم ها و پروژه ها و در نهایت تاخیر در تصمیم گیری اشاره کرد (داوودزاده، ۱۳۸۴).

۲. دلایل تلفیق مدیریت ریسک و مهندسی ارزش برای امنیت اطلاعات

اهمیت ملاحظات امنیتی در مورد توسعه و استفاده از سیستم های اطلاعاتی هیچ وقت از رشد بازمی ماند. در حقیقت، سیستم های اطلاعاتی امروزه در همه جا توسط افراد، سازمان ها، دولت ها و سیستم ها مورد استفاده قرار می گیرند و واضح است که این امر منجر به از دست دادن مقادیر زیادی پول، زمان و سایر منابع می شود. در نتیجه، سازمان ها ممکن است نه تنها میلیون ها دلار صرف تجهیزات امنیتی در برابر تهدیدات نمایند، بلکه با مشکلات زیادی برای ارزیابی بررسی های فناوری امنیتی مواجه هستند. به علاوه، این شرکت ها موارد امنیتی سیستم های آن ها را نقض می کنند چراکه سازمان هایی که بهتر ریسک های سایبری را مدیریت می کنند، از سوی بازار رقابتی مورد تقدیر قرار خواهند گرفت.

از سوی دیگر، کاربران سازمانی یا فردی انتظار دارند که سیستم های اطلاعاتی ایمن باشند و قادر به پیش بینی ریسک آن ها و استراتژی های آن ها در کاهش این ریسک ها باشند. هدایت اطلاعات سازمانی ایمن منجر به نیاز به توسعه بهتر معیارهای برای درک وضعیت نگرش امنیتی سازمان شده است.

محققان دلایل فراوانی برای تلفیق این دو رویکرد مطرح نموده اند که به برخی از آن ها اشاره می شود :

ارزش و ریسک مکمل یکدیگرند: برای بیشینه نمودن فرصت های موجود در امنیت سایبری، هر دو رویکرد مورد نیاز هستند. ارزش، با استفاده از رویکرد مدیریت ارزش بیشینه می گردد و هم راستا با آن عدم قطعیت و تهدیدها با کمک رویکرد مدیریت ریسک کمینه می شوند (دالاس، ۲۰۰۶).

۳. تعاریف کلیدی

- ❖ هزینه‌ی ریسک: هزینه‌ای که سازمان برای ریسک باید هزینه کند.
- ❖ احتمال وقوع ریسک: حد و اندازه‌ای که محتمل است یک واقعه رخ دهد .
- ❖ شدت تاثیر ریسک: اثر ریسک بیان کننده ی مقدار انحرافی است که در اثر وقوع ریسک در طول پروژه در هدفهای آن بوجود می آید. هر چه اثر ریسک بر هدف های پروژه بیشتر باشد شدت تاثیر آن بالاتر است .
- ❖ درجه سختی ریسک: حاصلضرب دو ملاک کمی شدت تاثیر و احتمال وقوع ریسک است (قراجورلو ، ۱۳۸۴).

۴. بیان مسئله

محرك‌هایی قوی برای پرداختن به ارزیابی ریسک امنیتی در دیدگاهی جدید ، مخصوصاً برای مدیریت ریسک امنیت اطلاعات وجود دارند. در حقیقت، فاکتورهای مشخصی وجود دارند که موجب تحریک تغییرات در شرکت می‌شود. برای مثال، استفاده از فناوری‌های جدید، فشار نوآوری و فشاری برای کاهش هزینه‌ها، شرکت‌ها را مجبور به در نظر گرفتن این جنبه‌ها می‌کند و صرف‌نظر از این فاکتورهای می‌تواند بر شهرت و اعتماد به نفس مشتری تأثیر بگذارد.

ارزیابی ریسک امنیت اطلاعات کاری مشکل و پرهزینه است. در حقیقت، اگر یک آسیب‌پذیری جدید یا یک ویروس جدید شناخته شود، این نتایج ممکن است بسیار هزینه‌بر باشند. علاوه بر این، برای فراهم آوری پاسخی سریع و مناسب به حوادث امنیتی و محافظت از دارایی‌هایی آنها، سازمان‌ها نیاز به یک رویکرد ارزیابی ریسک امنیتی نظام‌مند دارند. به‌علاوه، کاربران سازمانی یا فردی انتظار دارند که سیستم‌های اطلاعاتی ایمن باشند و قادر به پیش بینی ریسک آنها باشند و استراتژی‌های آنها این ریسک‌ها را کاهش دهد. هدایت اطلاعات سازمانی ایمن منجر به توسعه معیارهای بهتری برای درک وضعیت نگرش امنیتی سازمان شده است. از سوی دیگر، ارزیابی ریسک یکی از مؤلفه‌های پایه‌ای یک فرایند مدیریت ریسک سازمانی است. مبتنی بر معیارهای امنیتی برای ارزیابی ریسک‌های امنیتی می‌باشد. لذا در این مقاله تلاش شد تا ریسک های جدی سازمانی از لحاظ امنیت اطلاعات بر اساس مدیریت ارزش بررسی شود.

۵. روش تحقیق

بر اساس طرح پژوهش و از دید نحوه گردآوری داده ها، پژوهش حاضر از نوع توصیفی است و برای گردآوری اطلاعات سه روش مطالعه اسنادی و فرمول هزینه ریسک را به کار برده است. اطلاعات خبرگان به کمک پرسشنامه جمع آوری شده است. در پرسشنامه این پژوهش که با هدف کسب نظر خبرگان درباره ریسک های امنیت اطلاعات سازمانی طراحی شده است، از میان عوامل امنیت اطلاعات ۵۵ ریسک امنیتی استخراج شد که سرانجام در قالب ۱۵ ریسک امنیتی مشخص شد. در این پرسشنامه، هر یک از خبرگان نظر خود را درباره میزان ریسک تک تک عوامل برای امنیت اطلاعات در طیف پنج گانه لیکرت از طریق متغیرهای کلامی (خیلی کم، کم، متوسط، زیاد و خیلی زیاد) و با رویکردی مدیریت ارزش ابراز کردند.

۶. یافته ها

۶.۱. رویکرد تلفیقی مدیریت ریسک - مهندسی ارزش

در تعریف ارزش اگر عامل ریسک به درستی به کار گرفته شود نتایج مثبتی خواهد داشت. اسنودگرس رابطه ی زیر را در رابطه با ارزش ارائه کرده است:

$$(۱) \quad \text{تلاش ها} / (\text{عامل ریسک} \times \text{عملکرد}) = \text{ارزش}$$

با استفاده از این تعریف می توان رابطه ی مربوط به محاسبه ی شاخص ارزش را به شکل زیر بهبود بخشید:

$$(۲) \quad \text{عامل ریسک} = \frac{\text{هزینه ریسک}}{\text{بهای ریسک}} = \frac{\text{شاخص ارزش}}{\text{"بهبود شده"}}$$

برای رسیدن به اهداف مورد نظر هر تحقیق و پژوهش، استفاده از یک روش تحقیق علمی و نظام مند ضروری است. روش تحقیق مورد استفاده در این پژوهش «توصیفی» است. بدین منظور، سعی می شود از روش های کیفی به صورت توأمان استفاده شود و علاوه بر این، در گردآوری اطلاعات از روشهای متداول مانند بررسی کتابخانه ای و اسنادی، جستجوی اینترنتی استفاده شده است.

۶.۲. شناسایی عوامل ریسک در امنیت اطلاعاتی سازمانی :

به منظور افزایش اعتبار و قابلیت اعتماد نتایج این مطالعه برای کلیه ی پروژه های مشابه، پس از اجرای چند پرسشنامه ی نمونه، طراحی نهایی پرسشنامه ای باز پاسخ، صورت گرفت و اقدام به نظر سنجی از ۱۰ نفر از متخصصین و

کارشناسان اطلاعاتی در سازمان ها گردید. پس از تحلیل نظرات پاسخ دهندگان، ۱۵ عامل ریسک به شرح جدول ۱ مورد شناسایی، ارزیابی و اولویت بندی قرار گرفت.

جهت محاسبه ی درجه تأثیر می توان از این فرمول استفاده کرد:

$$\text{وزن عملکرد} \times \text{درجه عملکرد} + (\text{وزن ریسک} \times \text{درجه هزینه ریسک}) + (\text{وزن زمان} \times \text{درجه زمان}) = \text{درجه تأثیر}$$

برای تأثیر High عدد ۳، برای تأثیر Medium عدد ۲ و برای تأثیر Low عدد ۱ در نظر گرفته می شود و درجه ی تأثیر هر عامل را در وزن آن ضرب می شود.

جدول ۱. تاثیراتی که هر ریسک بر اساس ارزش بر سازمان دارد

ردیف سنجی	احتمال وقوع	شدت تأثیر	شرح عامل ریسک
۵/۹۵۰	۸۰	۸۰	۱ نبود خط مشی امنیت اطلاعات جامع و کامل و قابل بازنگری
۴/۵۰۰	۷۰	۹۰	۲ ناهماهنگی بخش های گوناگون بانک، در زمینه فعالیت های امنیت اطلاعات
۲/۸۰۰	۳۰	۲۰	۳ روشن نبودن تعریف مسئولیت امنیت اطلاعات در سازمان
۴/۸۰۰	۴۰	۴۰	۴ به کارنبردن رویه ای مناسب در طبقه بندی و کدگذاری اطلاعات
۱/۴۵۰	۴۰	۱۵	۵ ناهماهنگی سیستم ها با خط مشی ها و استانداردهای امنیتی
۱/۲۲۵	۷۰	۸۵	۶ همراستا نبودن فعالیت های امنیتی با نیازمندی های کسب و کار در سازمان
۱/۹۵۰	۵۰	۹۰	۷ مدیریت نادرست حوادث و ضعف های امنیت اطلاعات
۵/۶۰۰	۷۰	۴۰	۸ بی تعهدی و حمایت نکردن مدیریت سازمان درباره امنیت اطلاعات در سازمان
۶/۸۰۰	۸۰	۶۰	۹ تخصیص بودجه نامناسب به طرح امنیت
۸/۱۰۰	۳۰	۱۵	۱۰ بی توجهی در زمانبندی پیاده سازی و اجرایی کردن طرح ها
۵/۹۵۰	۳۵	۳۵	۱۱ بی بهرگی از طرح کلی برای امنیت اطلاعات و سرمایه گذاریهای مناسب و متناسب با اولویت های امنیتی
۴/۵۰۰	۳۰	۶۵	۱۲ بهره نبردن از نیروی انسانی متخصص در زمینه امنیت اطلاعات

۲/۸۰۰	۸۰	۷۰	ناآگاهی از امنیت اطلاعات و بی توجهی به آموزش آن	۱۳
۴/۸۰۰	۸۵	۸۰	مشخص نبودن راهی برای دسترسی های مناسب	۱۴
۰/۴۵۰	۹۰	۹۰	نامن بودن تجهیزات در برابر حوادث طبیعی و مصنوعی (نداشتن برق اضطراری، UPS و...)	۱۵

پس از شناسایی ریسک ها و محاسبه ی درجه سختی آن ها، طی برگزاری جلسه توفان مغزی، شدت تاثیر، احتمال وقوع و درجه سختی در جدول ۱ ارائه شد.

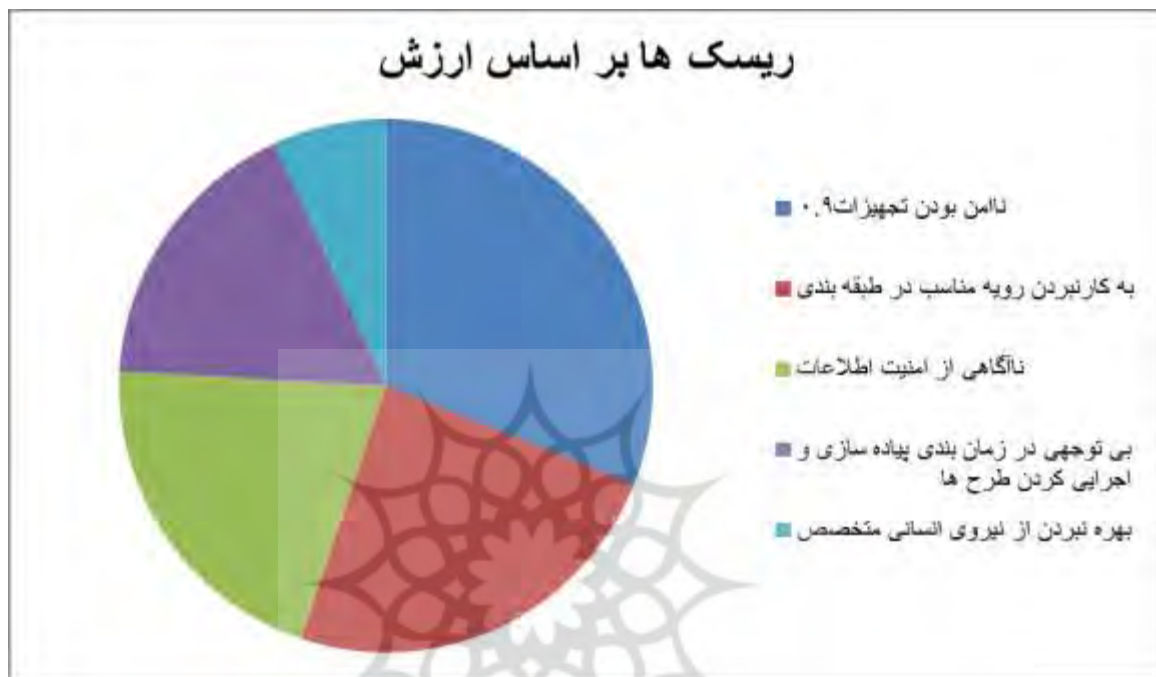
۶,۳. محاسبه عامل ریسک در رابطه با شاخص ارزش:

هر ریسک جدید می تواند یک فرصت و یا یک تهدید محسوب گردد. اگر ریسک جدید ایجاد فرصت نماید. اکنون با توجه به جدول تنظیم شده برای هر ایده برتر میانگین مقادیر درجه ی سختی ریسک به دست می آید که به معنای فشار و هزینه وارده بر سازمان به دلیل بی توجهی و آسیب ناشی از ریسک می باشد.

جدول ۳: اولویت بندی ریسک های جدید

درجه ی سختی ریسک	امتیاز ریسک	شرح عوامل ریسک شناسایی شده برای هر ایده	اولویت ریسک هر ایده	شماره ریسک هر ایده
۰/۹	بالا	نامن بودن تجهیزات در برابر حوادث طبیعی و مصنوعی (نداشتن برق اضطراری، UPS و...)	۱	۱
۰/۷	بالا	به کاربردن رویه ای مناسب در طبقه بندی و کدگذاری اطلاعات	۲	۱
۰/۶	متوسط	ناآگاهی از امنیت اطلاعات و بی توجهی به آموزش آن	۳	۲
۰/۵	متوسط	بی توجهی در زمانبندی پیاده سازی و اجرایی کردن طرح ها	۴	۲
۰/۲	کم	بهره نبردن از نیروی انسانی متخصص در زمینه امنیت اطلاعات	۵	۳
۰/۱	کم	روشن نبودن تعریف مسئولیت امنیت اطلاعات در سازمان	۶	۳

درجه سختی برای ناامن بودن تجهیزات در ردیف اول مهمترین و تاثیرگذارترین عوامل قرار گرفت و مشخص شد که این عامل ریسک بیشترین فشار را می تواند به سازمان وارد کند و در درجه دوم اهمیت "به کار نبردن رویه ای مناسب در طبقه بندی و کدگذاری" قرار دارد که این عوامل باید در هر سازمانی که با داده و امنیت اطلاعات کار دارند، مورد توجه قرار بگیرند.



ریسک های جدی سازمان بر اساس ارزش

۶.۴. بحث:

در حال حاضر، اطلاعات مهمترین گنجینه سازمان ها و اشخاص محسوب می شود و از بین رفتن و حتی کوچکترین آسیب به آن، نیازمند صرف زمان، هزینه و نیروی کار تصورناپذیری برای جبران است و در برخی مواقع اصول کاری و موجودیت یک سازمان را تهدید می کند. در این راستا، مدیریت امنیت اطلاعات برای ایجاد امنیت در پیدایش و تبادل اطلاعات، به کمک نظام مدیریتی بر پایه استانداردها و راهنماهای فنی و تصمیم های صحیح مدیریتی، می تواند موجب بهبود عملکرد نظام اطلاعاتی و ارتباطی شود. بنابراین ریسک های مرتبط با این فرایند باید کنترل شود. مدیریت ریسک ابزار خوبی برای کنترل ریسک است. به کارگیری روش های مدیریت و ارزیابی ریسک بر اساس مدیریت ارزش، تأثیر شگرفی بر چگونگی سروسامان دادن به فعالیت های سازمان ها در زمینه امنیت اطلاعات دارد. در مدیریت ریسک اولین و اساسی ترین گام، شناسایی ریسک است (موسوی و همکاران، ۱۳۹۴).

با پیدایش اولین استاندارد مدیریت امنیت اطلاعات در سال ۱۹۹۵، نگرش نظام مند به مقوله ایمن سازی فضای تبادل اطلاعات شکل گرفت (سانگو، لی و کیم، ۲۰۰۷). تصمیم گیری مناسب اولیه در زمینه مدیریت ریسک امنیت اطلاعات، می تواند هزینه ها را کاهش دهد و کنترل ریسک را سهولت بخشد. در تصمیم گیری های امنیتی، سطح بالایی از بی اطمینانی در مجموعه داده ها وجود دارد. به دلیل محدودیت های متعددی چون وقوع بعضی حوادث، ذهنیت بشر و ملاحظات اقتصادی، دستیابی به داده های کمی دشوار است و اگر هم داده هایی در دسترس باشند، اغلب نادرست اند یا به آنها نمی توان اطمینان کرد.

مدیریت امنیت اطلاعات از طریق استانداردها و سامانه های مدیریتی امنیت اطلاعات در سازمان ها اجرا می شود (مؤسسه استاندارد و تحقیقات صنعتی ایران، ۱۳۸۷) همچنین، مدیریت ریسک پروژه یکی از موضوعات عمده مدیریت پروژه است که برنامه ریزی، سازماندهی، پایش و کنترل تمام جنبه های پروژه را دربردارد و شامل شناسایی ریسک، اندازه گیری آن، توسعه پاسخ ریسک و کنترل پاسخ ریسک است (جعفرنژاد و یوسفی زنون، ۱۳۹۲). لذا شناسایی و ارزیابی ریسک، در اولویت بندی و ارائه راه حل صحیح برای اقدامات اصلاحی و پیشگیرانه نقش اساسی دارد. در این پژوهش، وارد کردن مهندسی ارزش در بررسی و ترجمه سختی هر ریسک برای هر سازمان، سبب قویتر شدن مرحله شناسایی ریسک شده است. این موضوع معیارهایی را بدست داد که می توان آن ها به عنوان ریسک های تأثیرگذار در سازمان های مختلف، گسترش داد.

نتایج پژوهش، ریسک های امنیت اطلاعات سازمانی را شناسایی و ارزیابی کرد. لذا به منظور کاهش و کنترل آنها، ارائه راهکارهای مدیریتی مبتنی بر مدیریت ریسک و ارزش، لازم به نظر می رسد. از سوی دیگر، ریسک هایی که نسبت به سایر ریسک ها برای سازمان مد نظر کمتر مطرح اند، به توجه و صرف زمان و هزینه کمتری نیاز دارند. با توجه به اینکه تلفیق مهندسی ریسک و ارزش علاوه بر کاهش زمان لازم برای پیش مطالعه و آنالیز ریسک و ارزش به صورت مجزا، میزان صرفه جویی هزینه و زمان بیشتری را به همراه خواهد داشت، سازمان ها می توانند از ریسک های معرفی شده در این پژوهش برای تقویت سیستم های امنیت اطلاعات برای مدیران در مدیریت ریسک امنیت اطلاعات، بهره ببرند. به این ترتیب بخش هایی از سازمان که به توجه، زمان و هزینه بیشتری نیاز دارند، مشخص می شود.

تاکید عمده گروه مدیریت ریسک بر روی هزینه های اولیه امنیت اطلاعات یعنی هزینه های تجهیزات و نیروی انسانی می باشد. درحالی که مهندسی ارزش همواره هزینه ی وارده بر سازمان را مورد بررسی قرار می دهد. از این رو کاربرد تلفیقی این دو روش در پروژه، دامنه دید کارفرما را در انتخاب گزینه ی مناسب گسترش می دهد. با توجه به اینکه مهم ترین بخش

امنیت یک سازمان، تقویت و پیشگیری پیش از آسیب است، چرا که غالباً هر گونه اصلاحی پس از خدشه دار شدن امنیت اطلاعات در سازمان نمی تواند چندان ثمربخش و مؤثر واقع شود، توجه به مدیریت ریسک، ریسک های بالا و هزینه هایی که به سازمان تحمیل می کنند که در بسیاری از موارد می تواند باعث کاهش چشمگیر آسیب پذیری ها شود یا پیامدهای یک تهدید را به حداقل ممکن کاهش دهد

۷. نتیجه گیری

در این پژوهش با هدف کسب نظر خبرگان درباره ریسک های امنیت اطلاعات سازمانی پرسشنامه بین خبرگان توزیع شد، از میان عوامل امنیت اطلاعات ۵۵ ریسک امنیتی استخراج شد که سرانجام در قالب ۱۵ ریسک امنیتی مشخص شد. در این پرسشنامه، هر یک از خبرگان نظر خود را درباره میزان ریسک تک تک عوامل برای امنیت اطلاعات در طیف پنج گانه لیکرت از طریق متغیرهای کلامی (خیلی کم، کم، متوسط، زیاد و خیلی زیاد) و با رویکردی مدیریت ارزش ابراز کردند. درجه تاثیر هزینه هر ریسک و سختی آن برای سازمان مشخص شد. در این مطالعه که مطالعه تطبیقی بین ریسک ها از نظر ارزش آن ها برای سازمان بود، یافته ها نشان داد عملکرد توأم مدیریت ریسک و مهندسی ارزش در امنیت سیستم های سایبری، با افزایش امنیت همراه خواهد بود بوده است. ارزیابی ریسک، مکانیزمی مهم در چرخه مدیریت امنیت اطلاعات است. برای شرکت ها جهت پذیرش یک فرایند به خوبی ساختاریافته و نظام مند جهت ارزیابی ریسک های امنیت اطلاعات جهت ارزیابی آن، اهمیت دارد. نتیجه نهایی این پژوهش این شد که نا امن بودن تجهیزات و به کار نبردن رویه های مناسب در طبقه بندی اطلاعات توسط نیروی انسانی از مهمترین علل ایجاد نا امنی در فضای اطلاعاتی و سایبری سازمان ها می باشند و توجه مدیران سازمانی به این ریسک ها می تواند از وارد شدن هزینه های مازاد به سازمان پیشگیری کند.

منابع

حسینی، محسن و ذکایی آشتیانی، سید حسین (۱۳۸۵). راهنمای گسترده دانش مدیریت پروژه (PMBOK) ویرایش سوم، چاپ اول، تهران: انتشارات آدینه.

داوود زاده، عرب؛ مهدی خانی، حسین و رضوی، سید مهدی (۱۳۸۴). ارتقای اثر بخشی مطالعات مهندسی ارزش با استفاده از مدیریت ریسک. تهران: دومین سمینار ملی مهندسی ارزش.

پریسا موسوی، رضا یوسفی زنوز، اکبر حسن پور، شناسایی ریسک های امنیت اطلاعات سازمانی با استفاده از روش دلفی فازی در صنعت بانکداری، مدیریت فناوری اطلاعات، دوره ۷، شماره ۱، بهار ۱۳۹۴

قراچارلو، نجف (۱۳۸۴). ارزیابی و مدیریت ریسک، چاپ اول، تهران: انتشارات علوم و فنون.

Dallas, Michael F. (۲۰۰۶). Maximizing Project Value Though Integrated Risk and Value Management. Retrieves June ۱۶, ۲۰۰۸, from Society of American Value Engineering. Website: www.value-eng.org/education and training/knowledge bank.

Feng, N., Jiannan Wang, H. & Li, M. (۲۰۱۴). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Information Sciences, ۲۵۶: ۵۷-۷۳.

Lo, Ch. & Chen, W. (۲۰۱۲). Hybrid information security risk assessment procedure considering interdependences between controls. Expert Systems with Applications, ۳۹: ۲۴۷-۲۵۷.

Chin, K.S., Tang, D.W., Wong, Sh. Y., Wang, H. (۲۰۰۹). Assessing new product development project risk by Bayesian network with a systematic probability generation methodology. Expert Systems with Applications, ۳۶ (۶): ۹۸۷۹- ۹۸۹۰.

Mireskandari, M. (۲۰۱۰). Information Security Management System and the necessity of its use in organizations. Processor magazine. ۱۱(۱۰۷): ۳۰-۳۹. (in Persian)

Jafarnejad, A. & yusefizenouz, R. (۲۰۰۸). The risk Ranking fuzzy Model in the drilling project of Petropars. Journal of Industrial Management of Tehran University, ۱(۱): ۲۱-۳۸. (in Persian)

Standard Institute and Industrial Research of Iran. (۲۰۰۸). IT- security technologies and information security management procedures. (in Persian)

Sungho, K, S., Jang, J.L. & Kim, S. (۲۰۰۷). Common defects in information security management system of Korean companies. The Journal of Systems and Software, ۸۰(۱۰): ۱۶۳۱-۱۶۳۸.