مجله پژوهش های معاصر در علوم و تحقیقات
سال اول، شماره ۴، آبان ۱۳۹۸
ISSN: ۲۶۷۶-۵۷۶٤
www.jocrisar.ir

مدیریت ریسک و ارزش در امنیت سایبری سازمانی

محمدامین صادقی[۱] ، حسین کارگر[۲] ، مهدی اکبری دهزیری[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 دارایی ها، قدرت و امنیت دانست و مهندسی ارزش، مدیریت ارزش بخشی جدایی ناپذیر از مدیریت ریسک به حساب می آید. یکپارچه سازی مهندسی ارزش و مدیریت ریسک باعث ایجاد هم افزایی می‌شود؛ این هم افزایی وقتی در امنیت سایبری پیاده شود، می تواند بر امنیت سایبری تاثیر بگذارد. این مقاله ارزیابی ریسک امنیت سایبری مبتنی بر ارزش، درجه تاثیر و درجه سختی بررسی می‌کند. دراین پژوهش بـا هدف کسب نظر خبرگان دربارۀ ریسک های امنیت اطلاعات سازمانی پرسشنامه بین خبرگان توزیع شد، از میان عوامل امنیت اطلاعات۵۵ ریسک امنیتی استخراج شد که سرانجام در قالـب ۱۵ ریسـک امنیتـی مشخص شد. در این پرسشنامه، هر یک از خبرگان که تعداد آنها ۱۰ نفر بود نظـر خـود را دربـارۀ میـزان ریسک تک تک عوامل برای امنیت اطلاعات در طیف پنج گانۀ 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 توام 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 دارایی ها و قدرت کسب درآمد دانست و مهندسی ارزش، مدیریت ارزش بخشی جدایی ناپذیر از مدیریت ریسک به حساب می آید. یک پارچه سازی مهندسی ارزش و مدیریت ریسک باعث ایجاد هم افزایی می‌شود. موضوع امنیت اطلاعات در سازمان ها، استفاده از سیستم های امنیت اطلاعـات را بـا چـالش ریسک مواجه کرده است. چنانچه فرایند مدیریت ریسک در این سیستم ها به درستی انجام شـود، می توان به اجرای موفق آن دست یافت (فنگ و همکاران،۲۰۱۴).

به طور کلی مدیریت ریسک شامل سـه گـام اساسـی شناسـایی ریسـک، ارزیـابی ریسـک و برنامه ریزی کاهش ریسک است. در شناسایی و تعیین میزان ریسک سیستم اطلاعاتی، مشکلاتی مانند نبود داده های آماری، موجب می‌شود مقـادیر نادرسـتی بـرای ریسـک سیسـتم اطلاعـاتی، محاسبه شود. از این رو اغلب روش‌های ارزیابی ریسک بـرای سیسـتم هـای اطلاعـاتی بـر پایـهٔ معیارهای کیفی بنا شدهاند نه معیارهای کمی. با این حال، ارزیابی کیفی ریسک بـرای شناسـایی ریسک‌ها تا حدودی ذهنی است. (لو و چن،۲۰۱۲).

موسسه ملی استاندارد و فناوری (NIST) مدیریت ریسک را به‌صورت "فرانید شناسایی ریسک، ارزیابی ریسک، و طی مراحلی برای کاهش ریسک به سطحی قابل‌قبول" تعریف می کند(میراسکندری، ۲۰۱۰). NIST ارزیابی ریسک را به‌صورت فرایند شناسایی، تخمین و اولویت‌بندی ریسک‌های امنیت اطلاعات تعریف می‌کند که نیازمند تحلیل دقیقی از تهدیدها و اطلاعات آسیب‌پذیری 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 امنیـت اطلاعـات هـر سـازمان، حفـظ سـرمایه هـای سـازمان (نـرم افـزاری، سخت افزاری، اطلاعاتی و ارتباطی و نیروی انسانی)در برابر هرگونه تهدید (دسترسی غیـر مجـاز به اطلاعات، خطرهای ناشی از محیط و سیستم و خطرهای ایجاد شده از سوی کاربران) اسـت و برای دستیابی به این اهداف به برنامهٔ منسـجمی نیـاز دارد. مـدیریت سیسـتم امنیـت اطلاعـات راهکاری برای رسیدن به این اهداف است ؟(چین و همکاران، ۲۰۰۹).

بهره‌گیری مجزا از دو رویکرد مهندسی ارزش و مدیریت ریسک در پروژه ها پیشینه ای طولانی دارد. تلفیق اثر بخش آنها مورد توجه پژوهشگران به ویژه دالاس(۲۰۰۶) قرار گرفته است. در این مقاله کوشش می شود تا الگویی ساده تر و کاربردی با محوریت بهینه سازی شاخص ارزش ایده های 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. درواقع، 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 اِعمال تغییرات پیشنهادی از یک سو و مسئولیت ایشان در قبال حوزه‌ی 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 ریسکِ 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 ارزش تر،رد گزینه های خلاقانه ، عدم تناسب ریسک درتصمیم‌ها و پروژه ها و درنهایت تاخیر درتصمیم 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 سیستم‌های اطلاعاتی هیچ‌وقت از رشد بازنمی‌ماند. در حقیقت، سیستم‌های اطلاعاتی امروزه در همه‌جا توسط افراد، سازمان‌ها، دولت‌ها و سیستم‌ها مورداستفاده قرار می‌گیرند و واضح است که این امر منجر به از دست دادن مقادیر زیادی پول، زمان و سایر منابع می‌شود. درنتیجه، سازمان‌ها ممکن است نه‌تنها میلیون‌ها دلار صرف تجهیزات امنیتی در برابر تهدیدات نمایند، بلکه با مشکلات زیادی برای ارزیابی بررسی‌های فناوری امنیتی مواجه هستند. به‌علاوه، این شرکت‌ها موارد امنیتی سیستم‌های آن‌ها را نقض می‌کنند چراکه سازمان‌هایی که بهتر ریسک‌های سایبری را مدیریت می‌کنند، از سوی بازار رقابتی موردتقدیر قرار خواهند گرفت.

از سوی دیگر، کاربران سازمانی یا فردی انتظار دارند که سیستم‌های اطلاعاتی ایمن باشند و قادر به‌پیش بینی ریسک آن‌ها و استراتژی‌های آن‌ها در کاهش این ریسک‌ها 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 تهدید ها با کمک رویکرد مدیریت ریسک کمینه می شوند(دالاس،۲۰۰۶).

۳. تعاریف کلیدی

- هزینه‌ی ریسک: هزینه ای که سازمان برای ریسک باید هزینه کند.
- احتمال وقوع ریسک: حد و اندازه ای 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 ملاکِ کمّی شدت تاثیر و احتمال وقوع ریسک است (قراجورلو ، ۱۳۸۴).

۴. بیان مسئله

محرک‌هایی 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 اعتمادبه‌نفس 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 به‌پیش 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 نحوۀ گردآوری داده ها، پژوهش حاضر از نـوع توصـیفی اسـت و برای گردآوری اطلاعات سه روش مطالعۀ اسنادی و فرمول هزینه ریسک را به کار برده است.اطلاعات خبرگان به کمک پرسشنامه جمع آوری شده است. در پرسشنامۀ این پژوهش کـه بـا هدف کسب نظر خبرگان دربارۀ ریسک های امنیت اطلاعات سازمانی طراحی شده است، از میان عوامل امنیت اطلاعات ۵۵ ریسک امنیتی استخراج شد که سرانجام در قالـب ۱۵ ریسـک امنیتـی مشخص شد. در این پرسشنامه، هر یک از خبرگان نظـر خـود را دربـارۀ میـزان ریسک تک تک عوامل برای امنیت اطلاعات در طیف پنج گانۀ 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:

ارزش = (عملکرد × عامل ریسک) / تلاش ها (۱)

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

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

بـــرای رســیـدن بـه اهـــداف مـــورد نظر هـر 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 هـای کیفی به صورت تـوأمـان اسـتـفـاده شـود و عـــلاوه بـر ایـــن، در گـــردآوری اطـلاعـات 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:

(وزن عملکرد× درجه عملکرد)+(وزن ریسک× درجه هزینه ریسک)+ (وزن زمان × درجه زمان)= 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

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

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

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.

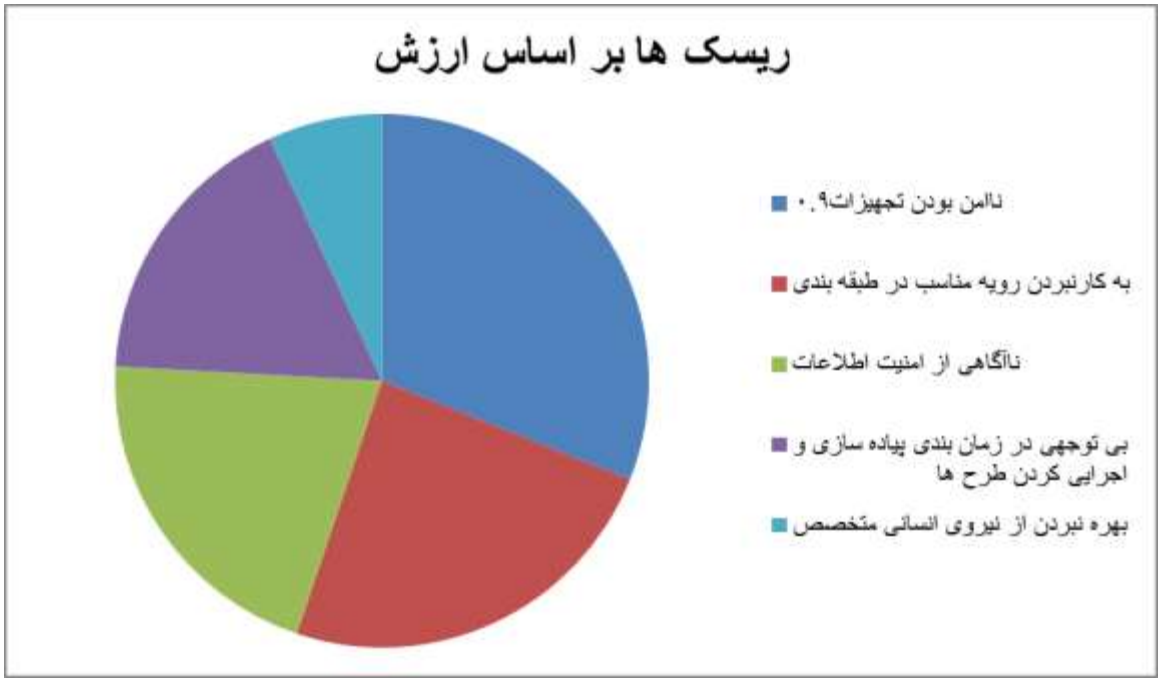
۶،۳. محاسبه عامل ریسک در رابطه با شاخص ارزش:

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 آیدکه 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

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

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 ازساس ارزش

۶,۴. بحث:

در حال حاضر، اطلاعات مهمترین گنجینهٔ سازمان ها و اشخاص محسوب می شود و از بین رفتن و حتی کوچکترین آسیب به آن، نیازمند صرف زمان، هزینه و نیروی کار تصورناپذیریی 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 پایهٔ 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 بایدکنترل 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 زمینهٔ 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 سال۱۹۹۵، نگرش نظام مند به مقولـۀ ایمن‌سازی فضای تبادل اطلاعات شکل گرفت (سانگو، لی و کیم ،۲۰۰۷). تصمیم گیری مناسب اولیه در زمینۀ مدیریت ریسک امنیت اطلاعات، مـی توانـد هزینـه هـا را کاهش دهد و کنترل ریسک را سهولت بخشد. در تصمیم گیـری هـای امنیتـی، سـطح بـالایی از بی اطمینانی در مجموعۀ داده ها وجود دارد. به دلیل محدودیت های متعـددی چـون وقـوع بعضـی حوادث، ذهنیت بشر و ملاحظات اقتصادی، دستیابی به داده های کمـی دشـوار اسـت و اگـر هـم داده هایی در دسترس باشند، اغلب نادرست اند یا به آنها نمی توان اطمینان کرد.

مـدیریت امنیت اطلاعات از طریق استانداردها و سامانه های مدیریتی امنیت اطلاعات در سـازمان هـا اجـرا می شود (مؤسسۀ استاندارد و تحقیقات صنعتی ایران،۱۳۸۷) همچنین، مدیریت ریسک پروژه یکی از موضوعات عمدۀ مدیریت پروژه است که برنامهریزی، سازماندهی، پایش و کنترل تمام جنبه های پروژه را دربردارد و شامل شناسایی ریسک، اندازهگیری آن، توسعۀ پاسخ ریسک و کنترل پاسخ ریسک است (جعفرنژاد و یوسفی زنوز،۱۳۹۲) .لـذا شناسـایی و ارزیـابی ریسـک، در اولویت بندی و ارائۀ راه حل صحیح برای اقدامات اصلاحی و پیشگیرانه نقش اساسی دارد. در ایـن پژوهش، وارد کردن مهندسی ارزش در بررسی و ئرجه سختی هر ریسک برای هر سازمان، سبب قویتر شدن مرحلۀ شناسایی ریسـک شـده است. این موضوع معیارهایی را بدست داد که می تـوان آن ها به عنوان ریسـک هـای تأثیرگذار در سازمان های مختلف، گسترش داد.

نتایج پژوهش، ریسک های امنیت اطلاعات سازمانی را شناسایی و ارزیابی کرد. لـذا به منظور کاهش و کنترل آنها، ارائۀ راهکارهای مدیریتی مبتنی بر مدیریت ریسک و ارزش، لازم بـه نظـر می رسد. از سوی دیگر، ریسک هایی که نسبت به سایر ریسک ها بـرای سـازمان مـد نظـر کمتـر مطرح اند، به توجه و صرف زمان و هزینۀ 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 سیسـتم هـای امنیت اطلاعات برای مدیران در مدیریت ریسک امنیت اطلاعات، بهره ببرند. به این ترتیب بخش هایی از سازمان که به توجه، زمان و هزینۀ 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 مهم‌ترین بخشِ

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 نمی‌تواند 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 مـوارد می تواند باعث کاهش چشمگیر آسیب پذیری ها شود یا پیامدهای یک تهدید را به حداقل ممکن کاهش دهد

۷. نتیجه‌گیری

در این پژوهش بـا هدف کسب نظر خبرگان دربارۀ ریسک های امنیت اطلاعات سازمانی پرسشنامه بین خبرگان توزیع شد، از میان عوامل امنیت اطلاعات۵۵ ریسک امنیتی استخراج شد که سرانجام در قالـب ۱۵ ریسـک امنیتـی مشخص شد. در این پرسشنامه، هر یک از خبرگان نظـر خـود را دربـارۀ میـزان ریسک تک تک عوامل برای امنیت اطلاعات در طیف پنج گانۀ 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 توام 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 شرکت‌ها جهت پذیرش یک فرایند به‌خوبی ساختاریافته و نظام‌مند جهت ارزیابی ریسک‌های امنیت اطلاعات جهت ارزیابی آن، اهمیت دارد. نتیجه نهایی این پژوهش این شد که نا امن بودن تجهیزات و به کارنبردن 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 هزینه‌های مازاد به سازمان پیشگیری کند.

منابع

حسینی، محسن و ذکایی آشتیانی، سید حسین (۱۳۸۵). راهنمای گستره دانش مدیریت پـروژه(PMBOK) ویـرایش سـوم، چاپ اول، تهران: انتشارات آدینه.

داوود زاده، عرب ؛ مهدی خانی، حسین و رضوی، سید مهدی(۱۳۸۴). ارتقای اثر بخشی مطالعات مهندسی ارزش با اسـتفاده 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، دورۀ ۷،شمارۀ ۱،بهـار 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. & yousefizenouz, 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 technologiesand 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.