نشریه علمی مطالعات مدیریت کسب و کار هوشمند- سال نهم ـ شماره ۳۴ـ زمستان ۱۳۹۹
مقاله پژوهشی/ صفحات ۲۱۴- ۱۹۱

Doi: 10.22054/IMS.2020.46866.1602

رویکردی ترکیبی از FMEA و تئوری خاکستری برای رتبه‌بندی ابعاد مدیریت ریسک امنیت اطلاعات

محسن شفیعی نیک‌آبادی *
سمانه طوقی **
امیرحکاکی ***

چکیده

پژوهش حاضر با هدف رتبه‌بندی هر یک از ابعاد مدیریت ریسک امنیت اطلاعات در سازمان‌ها انجام شده است. به همین منظور ابتدا با استفاده از مطالعه ادبیات پژوهش و نظرات خبرگان ابعاد و شاخص‌های مدیریت ریسک امنیت اطلاعات تعیین شده است. به‌منظور رتبه‌بندی عوامل مورد مطالعه با استفاده از رویکرد ترکیبیFMEA و تئوری خاکستری، ۵۰ پرسشنامه در میان کارشناسان صنعت IT که به‌صورت صورت قضاوتی-هدفمند انتخاب شده‌اند، توزیع و جمع‌آوری شده است. تجزیه‌وتحلیل نتایج نشان می‌دهد امنیت ارتباطات رتبه نخست اهمیت را به خود اختصاص می‌دهد. زیرساخت، عوامل انسانی، مدیریت امنیت، کنترل دسترسی به اطلاعات و توسعه‌ی سیستم‌های اطلاعاتی امن به ترتیب در رتبه‌های دوم تا ششم قرار گرفتند. با توجه به نتایج به دست آمده پیشنهاد می‌شود سازمان‌ها اقدام به ایجاد دپارتمان مستقل امنیت در سازمان نمایند. همچنین، تهیه فهرستی از کلیه‌ی دارایی‌های اطلاعاتی سازمان و مشخص نمودن اهداف کنترلی و راهبردی در حوزه امنیت اطلاعات در سازمان می‌تواند برای سازمان‌ها مفید باشد. اگر سازمانی دارای چندین شعبه است و نیاز به ارتباط از طریق اینترنت دارد، ترجیحاً ارتباطات به‌صورت VPN (رمزنگاری‌شده) برقرار گردد. درصورتی‌که سازمان خودکارسازی تحت وب دارد، این سایت می‌بایست مجهز به مجوزSSL و پروتکل https باشد.

کلید واژگان: مدیریت ریسک، امنیت اطلاعات، تئوری خاکستری، تجزیه تحلیل خطاهای بالقوه و اثرات آن، FMEA.

---

* عضو هیئت‌علمی، گروه مدیریت صنعتی، دانشکده اقتصاد، مدیریت و علوم اداری، دانشگاه سمنان، سمنان، ایران. (نویسنده مسئول)؛ shafiei@semnan.ac.ir

** کارشناس ارشد، گروه مدیریت صنعتی، دانشکده اقتصاد، مدیریت و علوم اداری، دانشگاه سمنان، سمنان، ایران.

*** دانشجوی دکتری، گروه مدیریت صنعتی، دانشکده اقتصاد، مدیریت و علوم اداری، دانشگاه سمنان، سمنان، ایران.

تاریخ دریافت: ۱۳۹۸/۰۷/۱۹ **تاریخ پذیرش**:۱۳۹۹/۰۳/۳۱

مقدمه

امروزه سازمان‌ها به دلیل تکامل و استفاده گسترده از اینترنت، اغلب در معرض انواع تهدیدها مانند دست‌کاری یا سرقت اطلاعات حیاتی قرار دارند. علاوه بر این، مشکلات طبیعی و خطاهای غیرعمدی که توسط کاربران رخ می‌دهد، می‌تواند نتایج مخربی را برای سازمان‌ها به بار آورد. این تهدیدها باعث اتلاف و تغییر در داده‌ها شده و بر روی خدمات و عملیات سازمان تأثیرگذار است. برای نمونه تخریب عملکرد در سرور ایستگاه کاری یا شبکه‌ها، آسیب به شبکه، نشت یا از دست دادن اطلاعات، زیان مالی (هزینه‌های بازیابی اطلاعات)، از دست دادن شهرت (اختلال در عملکرد کسب‌وکار) از جمله پیامدهای مهم تهدیدات مذکور است (حبیبی، ۱۳۹۷؛ حریری، ۱۳۹۱؛ سیلوا و همکاران[1]، ۲۰۱۴؛ شاو و همکاران[2]، ۲۰۰۹).

تجارت جهانی، شبکه‌ها و ظهور سازمان‌های مجازی از مهم‌ترین دلایل اهمیت یافتن امنیت اطلاعات است تا از آسیب به عملیات کسب‌وکار جلوگیری شود (فلورس و اکستدت[3]، ۲۰۱۶؛ شاملی–سندی و همکاران[4]، ۲۰۱۶). در حقیقت، فناوری اطلاعات هم فرصت است و هم تهدید! اگر به همان نسبتی که به توسعه آن توجه می‌کنیم به «امنیت» آن توجه نکنیم به‌سادگی تبدیل به یک تهدید بزرگ می‌شود. مطالعات نشان می‌دهد امروزه سازوکارهای امنیتی در سازمان به‌تنهایی اثربخشی چندانی ندارند زیرا امنیت اطلاعات در وهله اول مسئله انسانی و به همان میزان مسئله‌ای سازمانی یا مدیریتی است (اگوتچو و همکاران[5]، ۲۰۱۶؛ فنگ و وانگ[6]، ۲۰۱۴).

هم‌زمان با مطرح‌شدن شبکه‌های کامپیوتری و به دنبال آن اینترنت و در نتیجه گسترش استفاده از کامپیوترهای شخصی، کاربران ملزم به رعایت اصولی خاص و اهتمام جدی به تمامی مؤلفه‌های تأثیرگذار در تداوم ارائه خدمات می‌باشند. امنیت اطلاعات و ایمن‌سازی شبکه‌ها ازجمله این مؤلفه‌ها است که نمی‌توان آن را مختص یک فرد و یا سازمان دانست. پرداختن به

1. Silva et al.
2. Shaw et al.
3. Flores & Ekstedt
4. Shameli-Sendi et al.
5. Ogutcu et al.
6. Feng & Wang

مقوله امنیت اطلاعات در هر کشور، مستلزم توجه تمامی کاربران است چراکه وجود ضعف امنیتی در شبکه‌های کامپیوتری و اطلاعاتی، عدم آموزش و توجیه صحیح تمامی کاربران، عدم وجود دستورالعمل‌های لازم برای پیشگیری از نقایص امنیتی، عدم وجود سیاست‌های مشخص و مدون به‌منظور برخورد مناسب و به‌موقع با اشکالات امنیتی، مشکلاتی را به دنبال خواهد داشت که ضرر آن متوجه تمامی کاربران و سازمان است و تا حدی می‌تواند این مشکلات جدی باشد که عملاً زیرساخت اطلاعاتی یک کشور را در معرض تهدید قرار می‌دهد (نازارث و چوی[1]، ۲۰۱۵؛ وب و همکاران[2]، ۲۰۱۴؛ مهدی و وکیلی، ۱۳۹۷).

بر همین اساس حفاظت از سیستم‌های اطلاعاتی از حملات امنیتی برای بسیاری از سازمان‌ها به یک چالش مستمر تبدیل شده است (وینسنت و همکاران[3]، ۲۰۱۴). برخورداری از یک سیستم اولویت‌بندی عوامل مهم امنیت اطلاعات و اتخاذ تدابیر مناسب می‌تواند احتمال وقوع مخاطرات را به حداقل برساند و یا در صورت وقوع، میزان خسارت‌های وارده را بسیار ناچیزی نگه دارد. در حقیقت، تدابیر امنیتی موجب افزایش قابلیت واکنش سریع و مؤثر می‌شود و سازمان‌ها قادر خواهند بود برای ترمیم خسارت‌ها از فرایندهای از پیش تعیین شده استفاده کنند و بهره‌وری و ایمنی اطلاعات خود را افزایش داده و کسب‌وکار به‌صورت مطمئن‌تری تداوم یابد (شاملی-سندی و همکاران، ۲۰۱۶؛ فنگ و لی[4]، ۲۰۱۱). به همین منظور مدیریت سازمان همواره می‌بایست ضمن سیاست‌گذاری مشخص بر اساس اهداف کاری، پشتیبانی و تعهد خود به امنیت اطلاعات را از طریق انتشار و پایبندی به خط و مشی امنیت اطلاعات در کل سازمان به اثبات رساند (داویگا و مارتینز[5]، ۲۰۱۴).

FMEA یا تجزیه‌وتحلیل خطاهای بالقوه و اثرات آن یکی از جدیدترین روش‌هایی است که در کشورهای صنعتی مورد استفاده قرار می‌گیرد؛ این روش خطاهای ممکن و بالقوه را به‌طور سیستماتیک شناسایی نموده و ضرایب اولویت ریسک (RPN) کلیه خطاها را با

1. Nazareth & Choi
2. Webb et al.
3. Vicente et al.
4. Feng & Li
5. Da Veiga & Martins

ترکیب عواملی مانند شدت خطاها، نرخ وقوع خطاها و قابلیت کشف خطا، سنجیده و آنگاه با توجه به سیستم، اولویتی را جهت کاهش ریسک‌های موجود در طراحی و تولید محصولات جدید ارائه می‌دهد (حقیقی، ۱۳۷۹). همچنین، تئوری خاکستری یکی از مفاهیم ریاضی است که در مواجهه با مشکلات عدم اطمینان همراه با اطلاعات ناشناخته کاربرد دارد و استفاده از آن در سیستم‌های با اطلاعات ناقص در ۵ حوزه‌ی ارزیابی، مدل‌سازی، پیش‌بینی، تصمیم‌گیری و کنترل، روند رو به رشدی را دارد.

با ظهور خطرات بالقوه برای امنیت اطلاعات روش‌های مختلفی برای مدیریت ریسک امنیت اطلاعات و رتبه‌بندی ابعاد آن توسعه یافته‌اند و مطالعات بسیاری در حوزه مدیریت امنیت سیستم‌های اطلاعاتی انجام شده است. این در حالی است که تعداد کمی از این مطالعات بر ترکیب FMEA و امنیت اطلاعات متمرکز شده‌اند و مطالعه‌ای با استفاده از ترکیب FMEA و تئوری خاکستری برای رتبه‌بندی عوامل مشاهده نشده است. بر همین اساس، با توجه به موارد مطروحه و اهمیت مدیریت ریسک امنیت اطلاعات، پژوهش حاضر با هدف پاسخگویی به این سؤال است که "رتبه هر یک از ابعاد مدیریت ریسک امنیت اطلاعات با استفاده از رویکرد ترکیبی FMEA و تئوری خاکستری به چه میزان است؟" انجام شده است.

ادبیات پژوهش

مدیریت ریسک امنیت اطلاعات

امنیت اطلاعات، حفاظت اطلاعات و زیرساخت‌های فناوری، تضمین در دسترس بودن اطلاعات و به حداقل رساندن دسترسی‌های غیرمجاز تعریف می‌شود (شاملی- سندی و همکاران، ۲۰۱۶). مدیریت ریسک، فرآیندی است برای شناسایی مراحلی که باعث کاهش ریسک به یک تراز قابل‌قبول می‌شود (لی و همکاران[1]، ۲۰۰۷؛ آلبرت و دوروفی[2]، ۲۰۰۲). مدیریت ریسک امنیت اطلاعات عبارت است از شناسایی خطرات سازمانی و ارزیابی آسیبی که می‌تواند به سازمان وارد شود و تصمیم‌گیری برای کاهش خطر. مدیریت ریسک امنیت اطلاعات از دو جهت

1. Li et al.
2. Alberts & Dorofee

اهمیت دارد: ۱) خطراتی که عملیات سازمان را تهدید می‌کند کاهش می‌دهد. ۲) باعث یکپارچگی، محرمانگی و در دسترس بودن اطلاعات می‌شود (شامالا و همکاران[1]، ۲۰۱۳؛ متالیدو و همکاران[2]، ۲۰۱۴).

پیشینه پژوهش

در حوزه امنیت اطلاعات مطالعات گوناگونی در داخل و خارج کشور انجام شده که به مهم‌ترین آن‌ها اشاره می‌شود. به‌منظور ارائه مدلی برای رتبه‌بندی سازمان‌ها بر مبنای اندازه‌گیری و شناسایی میزان بلوغ امنیت اطلاعات در آن‌ها، پس از تعیین شاخص‌های امنیت اطلاعات در قالب دو دسته کلیِ فنی و مدیریتی و با توجه به معیارهای سه‌گانه امنیت، ایمنی و پایداری در سه سامان مورد مطالعه مشخص گردید از نظر بلوغ امنیت، بانک پاسارگاد رتبه اول را دارد. دانشگاه تهران و بانک تجارت در رتبه‌های بعدی قرار دارند (آرام، ۱۳۸۸). در پژوهشی دیگر با هدف شناسایی و مدل‌سازی سازه‌های مدیریتی مؤثر بر اثربخشی امنیت سیستم‌های اطلاعاتی، سازه‌های حمایت مدیریت عالی، آموزش امنیتی، فرهنگ امنیتی، مهارت امنیتی، تقویت خط‌مشی امنیتی، تجربیات و خودباوری افراد به‌عنوان عوامل مؤثر بر اثربخشی امنیت سیستم‌های اطلاعاتی معرفی شدند (زنده‌دل نوبری، ۱۳۸۹).

بررسی تأثیر عواملی که اطلاعات سازمان‌ها را با خطر سرقت، نابودی و یا تغییر اطلاعات مواجه می‌سازند نشان می‌دهد که مؤلفه آگاهی نداشتن کاربران بالاترین تهدید و پس‌ازآن امنیت نیروی انسانی دومین تهدید برای امنیت اطلاعات سیستم‌های رایانه‌ای است (طاهری، ۱۳۸۶). در سال ۲۰۱۶ مدلی برای تجزیه تحلیل ریسک امنیت اطلاعات با استفاده از تئوری تصمیم‌گیری فازی ارائه گردید که ترکیبی از تئوری تصمیم‌گیری و منطق فازی است (ساید و همکاران[3]، ۲۰۱۴). در پژوهشی دیگر با هدف ارائه یک رویکرد برای مدیریت ریسک امنیت اطلاعات، ۵ بعد معرفی گردید که عبارت‌اند از: دسترسی به اطلاعات و سیستم‌ها، امنیت ارتباطات،

1. Shamala et al.
2. Metalidou et al.
3. Said et al.

زیرساخت، توسعه سیستم‌های اطلاعاتی امن و مدیریت امنیت. این پژوهش بر اساس FMEA و تئوری فازی نشان می‌دهد امنیت ارتباطات و زیرساخت بیشترین ریسک را برای امنیت اطلاعات سازمان به همراه دارد (حبیبی، ۱۳۹۷).

بر اساس نتایج به دست آمده از پژوهش پیشین، مرحله‌ی مقدماتی مدیریت ریسک، تجزیه تحلیل ریسک است که به‌عنوان استفاده‌ی سیستماتیک از اطلاعات برای شناسایی منابع خطر تعریف می‌شود. اگر این مرحله به‌خوبی انجام نشود، انتخاب اقدام متقابل با شکست مواجه خواهد شد و مدیریت ریسک موفق نخواهد بود. گام‌های اساسی برای ارزیابی ریسک عبارت‌اند از: تعیین اثر بالقوه‌ی ریسک‌ها، ارزیابی احتمال وقوع و تأثیری که در نتیجه می-گذارند (گوسمائوو و همکاران[1]، ۲۰۱۶). در پژوهشی دیگر در سال ۲۰۱۳ با هدف مطالعه آگاهی از امنیت اطلاعات از منظر مدیران سیستم و کاربران نهایی در دانشگاه فلوریدا مشخص گردید عوامل انسانی در امنیت اطلاعات اهمیت ویژه‌ای دارند. همچنین مشخص می‌نماید مدیران سیستم تأکید بیشتری بر تهدیدهای خارجی و فنی نسبت به تهدیدهای داخلی دارند و کاربران نهایی نیاز به آموزش دارند تا بتوانند از خود در برابر تهدیدهای امنیتی محافظت کنند (گئو[2]، ۲۰۱۳). مطالعه آسیب‌پذیری امنیت در کتابخانه‌های دیجیتالی اروپا نشان می‌دهد اکثر کتابخانه‌های دیجیتالی نقص امنیتی جدی در برنامه‌های کاربردی تحت وب خود دارند. اکثر کتابخانه‌های اروپای غربی، مشکلات امنیتی بحرانی (۲۵٪) و یا در سطح متوسط (۴۰٪) داشتند. همچنین، کتابدارن اقدام‌های لازم برای ایمن‌سازی سیستم‌های اطلاعاتی آنلاین را اجرا نمی‌کنند (کوزما[3]، ۲۰۱۰). با هدف مطالعه رابطه سیستم‌های سازمان و آگاهی امنیت اطلاعات با تمرکز بر روی بررسی رابطه حیاتی بین سیستم‌های سازمان در چارچوب نظریه رفتار سازمانی و آگاهی امنیت اطلاعات (ISA) مشخص گردید آگاهی کاربران از امنیت اطلاعات با ساختار سازمان، فرهنگ‌سازمانی، روش‌ها و سیاست‌های منابع انسانی ارتباط معناداری دارد (مهابی[4]، ۲۰۱۰).

پژوهش‌های پیشین در حوزه مدیریت امنیت سیستم‌های اطلاعاتی نشان می‌دهد که اغلب از روش‌های تئوری فازی و روش‌های تصمیم‌گیری چند معیاره برای ارزیابی ریسک امنیت اطلاعات استفاده شده است. در این تحقیق تلاش می‌شود با ایجاد مدلی ۶ بعدی از امنیت

1. Gusmao et al.
2. Guo
3. Kuzma
4. Mahabi

اطلاعات بر اساس پژوهش‌های پیشین، با استفاده از ترکیب رویکرد FMEA با تئوری خاکستری کاستی‌های تحقیقاتی در این زمینه پوشش داده شود. جدول ۱ ابعاد و شاخص‌های هر بعد را با توجه به مرور ادبیات مرتبط نشان می‌دهد. به‌منظور درک بهتر به هر بعد یک علامت اختصاری اختصاص می‌شود.

جدول ۴: ابعاد و شاخص‌های امنیت اطلاعات

ابعاد	شاخص‌ها	منبع	ابعاد	شاخص‌ها	منبع
کنترل دسترسی به اطلاعات و سیستم‌ها (A)	۱. عدم مدیریت رسانه‌های قابل‌حمل مانند فلش	حبیبی (۱۳۹۷)	امنیت ارتباطات (B)	۱. پست الکترونیکی ناامن	حبیبی (۱۳۹۷)
	۲. عدم کنترل رمز عبور			۲. عدم امنیت سیستم‌های اداری الکترونیکی	آلبرتس و دوروفی (۲۰۰۲)
	۳. عدم ثبت‌نام کاربر			۳. مدیریت رمزگذاری	
	۴. عدم به رسمیت شناختن پایانه خودکار			۴. عدم دسترسی محدود به محتوای اینترنت	فلورس و اکستدت (۲۰۱۶) فنگ و وانگ (۲۰۱۴)
	۵. عدم احراز هویت شناسه کاربر	طاهری (۱۳۸۶) پورمند (۱۳۸۵)		۵. عدم توجه به تهدیدات Instant Messaging	
	۶. عدم مدیریت دسترسی از بیرون به داخل سیستم			۶. استفاده راحت کارکنان از گوشی‌های هوشمند	
	۷. عدم شناسنامه‌دار نمودن دستگاه‌ها			۷. استفاده از گوشی‌های دوربین‌دار	
	۸. نداشتن رمز پیچیده			۸ استفاده از VOIP	
	۹. عدم تأکید بر تغییر رمز به‌صورت دوره‌ای			۹. استفاده از سیستم‌های غیر امن برای انتقال داده	گوسمائو و همکاران (۲۰۱۶)
	۱۰. عدم کنترل و ایجاد محدودیت تردد کارکنان			۱۰. کپی کردن راحت اطلاعات حساس	
	۱۱. عدم امنیت تجهیزات کاربر در غیاب کاربر	نظر خبرگان		۱۱. استفاده از نرم‌افزارهای بدون مجوز	
	۱۲. عدم محدودیت زمانی و مدت اتصال به شبکه		مدیریت امنیت (D)	۱. عدم وجود ممیزی امنیت اطلاعات	حبیبی (۱۳۹۷)
	۱۳. عدم جداسازی سیستم‌های خاص			۲. عدم وجود خط‌مشی برای امنیت اطلاعات	
	۱۴. عدم جداسازی شبکه‌ها			۳. عدم مسئولیت‌پذیری برای امنیت اطلاعات	لی و همکاران (۲۰۰۷)

زیرساخت (سخت‌افزار/ شبکه) (C)	۱. عدم پشتیبان گیری از اطلاعات	فلورس و اکستدت (۲۰۱۶) فنگ و وانگ (۲۰۱۴)		۴. عدم پشتیبانی از سخت‌افزار و نرم‌افزار	آلبرتس و دوروفی (۲۰۰۲)
	۲. عدم صدور گواهینامه برای گره‌های شبکه	اگوتچو و همکاران (۲۰۱۶)		۵. عدم بازنگری سیاست امنیت اطلاعات اجراشده	
	۳. عدم وجود اصالت نرم‌افزار	آلبرتس و دوروفی (۲۰۰۲)		۶. دور زدن مکانیسم‌های امنیتی توسط کاربران	
	۴. عدم دفاع ایمنی نرم‌افزار	وب و همکاران (۲۰۱۴)		۷. عدم ارائه مشوق‌های بازدارنده	وب و همکاران (۲۰۱۴)
	۵. عدم وجود سرور خوشه (cluster server)	گئو (۲۰۱۳) کوزما (۲۰۱۰) مهابی (۲۰۱۰)		۸. عدم پالایش سیاست‌های امنیتی	وب و همکاران (۲۰۱۴)
	۶. عدم وجود مولد الکترونیکی بازیابی		عامل‌های انسانی (F)	۱. عدم توجه به آگاهی و آموزش امنیت اطلاعات	طاهری (۱۳۸۶) پورمند (۱۳۸۵) محمود زاده (۱۳۸۵)
	۷. عدم مجزا سازی فضای آدرس			۲. عدم توجه به فرهنگ امنیت اطلاعات	
	۸. فیلتر نکردن پورت‌ها			۳. آگاه نبودن کارکنان از وظایف شغلی	
	۹. عدم کنترل ترافیک			۴. عدم تشریح مسئولیت-های امنیتی	
	۱۰. عدم امکان جداسازی داده‌های حساس			۵. عدم‌حمایت مدیران	
توسعه سیستم اطلاعاتی امن (E)	۱. شکست آزمون در برابر آسیب‌پذیری نرم‌افزار	داویگا و مارتینز (۲۰۱۴)		۶. دخالت مدیران در تصمیمات امنیت اطلاعات	
	۲. عدم‌تغییر فرایند کنترل ورود به سیستم				

تجزیه‌وتحلیل حالات شکست و اثرات آن

تجزیه تحلیل حالات شکست و اثرات آن (FMEA) برای شناسایی حالات بالقوه شکست، علل، اثرات، مشکلات مؤثر بر موفقیت سیستم، قابلیت اطمینان سخت‌افزار و نرم‌افزار، نگهداشت و

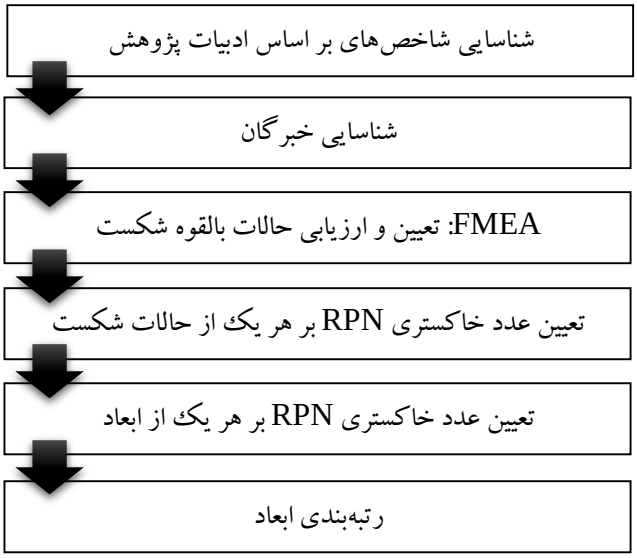
ایمنی سیستم است. FMEA با تجزیه تحلیل کل سیستم شروع و سپس زیرسیستم‌ها را بررسی می‌کند؛ عناصر آن عبارت است از: حالات بالقوه شکست و دلایل؛ اثرات بالقوه شکست؛ تشخیص شکست و جبران خسارت (اصلاح شکست‌ها) و رتبه‌بندی بر اساس شدت مورد انتظار از شکست (S)، احتمال وقوع حالت شکست (O)، تشخیص خطر قبل از آنکه بر مشتری اثر بگذارد (D) (حبیبی، ۱۳۹۷).

تئوری خاکستری

تئوری خاکستری در سال ۱۹۸۲ توسط دنگ مطرح گردید و به‌عنوان یکی از مفاهیم ریاضی در تصمیم‌گیری چند معیاره بسیار مؤثر در مواجهه با مشکلات عدم اطمینان همراه با اطلاعات ناشناخته است. مجموعه خاکستری مجموعه‌ای از داده‌های غیرقطعی است که به‌وسیله اعداد، معادلات و ماتریس‌های خاکستری تعریف می‌شوند. این رویکرد دو مزیت نسبت به سایر روش-ها دارد: ۱) نیاز به داده‌های کم. ۲) توانایی مواجهه با ابهام در داده‌ها. عدد خاکستری به‌عنوان عددی با اطلاعات نامطمئن است که با بازه‌ای که مقدار آن را در بر می‌گیرد شناخته می‌شود $\otimes \in [a,b]$ (الهی، ۱۳۸۷).

روش‌شناسی پژوهش

پژوهش حاضر از لحاظ هدف کاربردی با متغیر کیفی و از دید ماهیت در دسته پژوهش‌های توصیفی-تحلیلی قرار می‌گیرد که به‌صورت پیمایشی انجام شده است. هدف تحقیق بررسی رتبه هر یک از ابعاد مدیریت ریسک امنیت اطلاعات با استفاده از FMEA و تئوری خاکستری است. شکل ۱ مراحل انجام پژوهش را نشان می‌دهد.



شکل ۱: مراحل انجام پژوهش

مطابق با شکل ۱، در نخستین گام با استفاده از مطالعات کتابخانه‌ای و نظرات خبرگان صنعت IT در قالب مصاحبه باز شاخص‌ها پژوهش استخراج شده است. در ادامه داده‌های لازم برای رتبه‌بندی هر یک از ابعاد پژوهش با استفاده از پرسشنامه جمع‌آوری‌شده که روایی ظاهری و محتوایی آن بر اساس نظرات اساتید و خبرگان مورد تائید قرار می‌گیرد. با هدف تعیین و ارزیابی حالات بالقوه شکست در روش FMEA ابتدا عدد RPN برای هر شاخص مطابق با رابطه ۱ محاسبه می‌شود.

$$RPN=O*S*D \qquad \text{رابطه (۱)}$$

برای محاسبه عدد RPN هر بعد، اعداد RPN شاخص‌های مربوط به هر بعد با یکدیگر جمع می‌شوند تا در نهایت ابعاد مورد مطالعه بر اساس آن رتبه‌بندی شوند. هر چه عدد RPN به دست آمده بیشتر باشد، آن بعد ریسک بیشتری به دنبال دارد [۲]. پژوهش حاضر در بررسی RPN از طیف لیکرت ۷ تایی برای ارزیابی عوامل O، S و D استفاده می‌کند که به دلیل عدم

اطمینان و ناکامل بودن اطلاعات با توجه به تئوری خاکستری، قبل از محاسبه روابط ریاضی این مقیاس به بازه‌های خاکستری مطابق با جدول ۲ تبدیل می‌شود (الهی، ۱۳۸۷).

جدول ۵: عبارات کلامی و اعداد خاکستری متناظر

عبارت کلامی	مقدار	اهمیت
خیلی ضعیف	(۰-۱)	(۰/۰ – ۰/۱)
ضعیف	(۱-۳)	(۰/۱ – ۰/۳)
نسبتاً ضعیف	(۳-۴)	(۰/۳ – ۰/۴)
متوسط	(۴-۵)	(۰/۴ – ۰/۵)
نسبتاً قوی	(۵-۶)	(۰/۵ – ۰/۶)
قوی	(۶-۹)	(۰/۶ – ۰/۹)
خیلی قوی	(۹-۱۰)	(۰/۹ – ۱/۰)

مطابق با جدول ۲، اعداد به دست آمده برای O، S و D را به بازه‌های خاکستری تبدیل نموده و سپس از ضرب خاکستری برای محاسبه عدد RPN هر شاخص استفاده می‌شود (با فرض دو عدد خاکستری A و B مطابق با رابطه ۲ داریم). همچنین برای به دست آوردن عدد RPNهر بعد، از جمع خاکستری استفاده می‌شود

$$A=\{a,b\} \qquad B=\{c,d\} \quad \text{(رابطه ۳)}$$

$$A*B=\{\min(ac,ad,bc,bd),\max(ac,ad,bc,bd)\} \quad \text{رابطه (۲)}$$

$$A+B=\{a+c,b+d\} \quad \text{رابطه (۳)}$$

جامعه آماری تحقیق شامل کارشناسان صنعتIT، نرم‌افزار و شبکه بوده که دارای حداقل ۵ سال سابقه کاری و تحصیلات مرتبط با این حوزه باشند. حجم نمونه آماری ۵۰ نفر در

نظر گرفته شده است که به‌صورت قضاوتی-هدفمند و در دسترس انتخاب شده‌اند. جدول ۳ وضعیت جمعیت شناختی نمونه آماری پژوهش را نشان می‌دهد.

جدول ۶: وضعیت جمعیت شناختی نمونه آماری

مشخصات توصیفی		درصد توزیع
تحصیلات	کارشناسی	۳۸
	کارشناسی ارشد	۵۶
	دکتری	۶
سابقه کار	۵ – ۷ سال	۶۲
	۷ – ۱۰ سال	۳۰
	بالاتر از ۱۰ سال	۸

یافته‌های پژوهش

پژوهش حاضر با هدف رتبه‌بندی ابعاد و شاخص‌های امنیت اطلاعات در گام نخست از پرسشنامه‌ها برای هر سه عامل O، S و D میانگین گرفته شده است. سپس عبارات کلامی استخراج شده از پرسشنامه‌ها به بازه‌های عددی در طیف خاکستری تبدیل شده است؛ نکته قابل‌توجه در این مرحله این است که برای احتمال وقوع و شدت خطر، بازه‌ی عددی با عبارت کلامی رابطه‌ی مستقیم دارد (مثال: خیلی زیاد برابر است با بازه‌ی (۱۰-۹))؛ اما برای احتمال کشف، بازه‌ی عددی با عبارت کلامی رابطه‌ی معکوس دارد (مثال: خیلی زیاد برابر است با بازه‌ی (۱-۰)). جدول ۱۰ اعداد خاکستری برای هر شاخص و بعد را نشان می‌دهد.

جدول ۷: بازه خاکستری شاخص‌های ابعاد مورد مطالعه

ابعاد	شاخص	O	S	D	بازه خاکستری	ابعاد	شاخص	O	S	D	بازه خاکستری
کنترل دسترسی به اطلاعات و سیستم‌ها (A)	A_1	(۶-۹)	(۶-۹)	(۴-۵)	[۱۴۴ ۴۰۵]	امنیت ارتباطات (B)	B_1	(۴-۵)	(۶-۹)	(۴-۵)	[۹۶ ۲۲۵]
	A_2	(۴-۵)	(۶-۹)	(۴-۵)	[۹۶ ۲۲۵]		B_2	(۴-۵)	(۶-۹)	(۴-۵)	[۹۶ ۲۲۵]
	A_3	(۳-۴)	(۵-۶)	(۳-۴)	[۴۵ ۹۶]		B_3	(۴-۵)	(۶-۹)	(۳-۴)	[۷۳ ۱۳۵]
	A_4	(۵-۶)	(۴-۵)	(۵-۶)	[۳۶ ۸۰]		B_4	(۵-۶)	(۴-۵)	(۴-۵)	[۸۰ ۱۵۰]
	A_5	(۳-۴)	(۶-۹)	(۳-۴)	[۵۵ ۱۴۴]		B_5	(۵-۶)	(۵-۶)	(۴-۵)	[۱۰۰ ۱۸۰]
	A_6	(۳-۴)	(۶-۹)	(۳-۴)	[۵۵ ۱۴۴]		B_6	(۹-۱۰)	(۳-۴)	(۳-۴)	[۱۳۵ ۲۴۰]
	A_7	(۴-۵)	(۴-۵)	(۴-۵)	[۶۴ ۱۲۵]		B_7	(۹-۱۰)	(۶-۹)	(۳-۴)	[۱۶۲ ۳۶۰]
	A_8	(۵-۶)	(۴-۵)	(۴-۵)	[۸۰ ۱۵۰]		B_8	(۴-۵)	(۳-۴)	(۴-۵)	[۴۸ ۱۰۰]
	A_9	(۴-۵)	(۵-۶)	(۴-۵)	[۸۰ ۱۵۰]		B_9	(۵-۶)	(۶-۹)	(۴-۵)	[۱۲۰ ۲۷۰]
	A_{10}	(۳-۴)	(۶-۹)	(۳-۴)	[۵۴ ۱۴۴]		B_{10}	(۶-۹)	(۶-۹)	(۵-۶)	[۱۸۰ ۴۸۶]
	A_{11}	(۴-۵)	(۶-۹)	(۴-۵)	[۹۶ ۲۲۵]		B_{11}	(۵-۶)	(۶-۹)	(۴-۵)	[۱۲۰ ۲۷۰]
	A_{12}	(۵-۶)	(۳-۴)	(۳-۴)	[۴۵ ۹۶]	مدیریت امنیت (D)	D_1	(۵-۶)	(۵-۶)	(۴-۵)	[۱۰۰ ۱۸۰]
	A_{13}	(۴-۵)	(۵-۶)	(۳-۴)	[۶۰ ۱۲۰]		D_2	(۳-۴)	(۶-۹)	(۳-۴)	[۵۴ ۱۴۴]
	A_{14}	(۴-۵)	(۵-۶)	(۳-۴)	[۶۰ ۱۲۰]		D_3	(۴-۵)	(۶-۹)	(۴-۵)	[۹۶ ۲۲۵]
زیرساخت (سخت‌افزار/ شبکه) (C)	C_1	(۴-۵)	(۶-۹)	(۴-۵)	[۹۶ ۲۲۵]		D_4	(۳-۴)	(۶-۹)	(۳-۴)	[۵۴ ۱۴۴]
	C_2	(۵-۶)	(۴-۵)	(۴-۵)	[۸۰ ۱۵۰]		D_5	(۴-۵)	(۵-۶)	(۴-۵)	[۸۰ ۱۵۰]
	C_3	(۶-۹)	(۵-۶)	(۳-۴)	[۹۰ ۲۱۶]		D_6	(۴-۵)	(۶-۹)	(۴-۵)	[۹۶ ۲۲۵]
	C_4	(۴-۵)	(۶-۹)	(۴-۵)	[۹۶ ۲۲۵]		D_7	(۴-۵)	(۳-۴)	(۴-۵)	[۴۸ ۱۰۰]
	C_5	(۴-۵)	(۵-۶)	(۴-۵)	[۸۰ ۱۵۰]		D_8	(۴-۵)	(۵-۶)	(۵-۶)	[۱۰۰ ۱۸۰]
	C_6	(۴-۵)	(۶-۹)	(۴-۵)	[۷۲ ۱۸۰]	عامل‌های انسانی (F)	F_1	(۴-۵)	(۶-۹)	(۴-۵)	[۷۲ ۱۸۰]
	C_7	(۴-۵)	(۵-۶)	(۳-۴)	[۶۰ ۱۲۰]		F_2	(۵-۶)	(۵-۶)	(۴-۵)	[۱۰۰ ۱۸۰]
	C_8	(۵-۶)	(۶-۹)	(۴-۵)	[۱۲۰ ۲۷۰]		F_3	(۳-۴)	(۶-۹)	(۳-۴)	[۵۴ ۱۴۴]
	C_9	(۴-۵)	(۵-۶)	(۳-۴)	[۶۰ ۱۲۰]		F_4	(۴-۵)	(۶-۹)	(۳-۴)	[۷۲ ۱۸۰]
	C_{10}	(۴-۵)	(۶-۹)	(۴-۵)	[۹۶ ۲۲۵]		F_5	(۴-۵)	(۶-۹)	(۴-۵)	[۹۶ ۲۲۵]
توسعه سیستم اطلاعاتی امن (E)	E_1	(۴-۵)	(۵-۶)	(۴-۵)	[۸۰ ۱۵۰]		F_6	(۵-۶)	(۵-۶)	(۴-۵)	[۱۰۰ ۱۸۰]
	E_2	(۴-۵)	(۵-۶)	(۳-۴)	[۶۰ ۱۲۰]						

پس از محاسبه بازه خاکستری هر یک از شاخص‌ها در ابعاد مورد مطالعه، با استفاده از رابطه ۳ بازه خاکستری هر یک از ابعاد مطابق با جدول ۵ محاسبه می‌گردد.

جدول ۸: بازه خاکستری هر یک از ابعاد مورد مطالعه

بعد (نماد)	بازه خاکستری
کنترل دسترسی به اطلاعات و سیستم‌ها (A)	[۹۶۸ ۲۲۲۴]
امنیت ارتباطات (B)	[۱۲۰۹ ۲۶۴۱]
زیرساخت سخت‌افزار و شبکه (C)	[۸۵۰ ۱۸۸۱]
مدیریت امنیت (D)	[۶۲۸ ۱۳۴۸]
توسعه سیستم اطلاعاتی امن (E)	[۱۴۰ ۲۷۰]
عامل‌های انسانی (F)	[۴۹۴ ۱۰۸۹]

پس از محاسبه اعداد RPN هر شش بعد مطابق (جدول ۵)، میانگین هر یک از این شش بازه را حساب کرده و در تعدیل گر α (تعداد شاخص‌های بعد تقسیم بر تعداد کل شاخص‌ها) ضرب می‌کنیم تا اثر تعداد شاخص‌های ابعاد بر رتبه‌ی آن‌ها را از بین ببریم. هر چه عدد RPN یک بعد بیشتر باشد، آن بعد ریسک بیشتری را به دنبال خواهد داشت. برای مثال برای کنترل دسترسی به اطلاعات و سیستم‌ها (A) داریم:

RPN (A) = [۹۶۸ ۲۲۲۴]

RPN (A) = (۹۶۸ +۲۲۲۴) / ۲ = ۱۵۹۶

α * A = ۵۱/۱۴

RPN (A) =۱۵۹۶ * α =۱۵۹۶ * (۵۱/۱۴) = ۵۸۱۴

با محاسبه RPN کل ابعاد و شاخص، رتبه به دست آمده ابعاد و شاخص‌های آن‌ها مطابق با جدول ۶ به دست می‌آید.

جدول ۹: رتبه‌بندی ابعاد امنیت اطلاعات و شاخص‌های هر یک از آن‌ها

ابعاد	شاخص‌ها	RPN	رتبه	ابعاد	شاخص‌ها	RPN	رتبه
امنیت ارتباطات (رتبه ۱)	کپی کردن راحت اطلاعات حساس	۳۳۳	۱	مدیریت امنیت (رتبه ۴)	عدم مسئولیت‌پذیری برای امنیت اطلاعات	۱۶۰/۵	۱
	استفاده از گوشی‌های دوربین‌دار	۲۶۱	۲		دور زدن مکانیسم‌های امنیتی توسط کاربران	۱۶۰/۵	۲
	استفاده از سیستم‌های غیر امن برای انتقال داده	۱۹۵	۳		عدم وجود ممیزی امنیت اطلاعات	۱۴۰	۳
	استفاده از نرم‌افزارهای بدون مجوز	۱۹۵	۴		عدم پالایش سیاست‌های امنیتی	۱۴۰	۴
	استفاده کارکنان از گوشی‌های هوشمند	۱۸۷/۵	۵		عدم بازنگری سیاست امنیت اطلاعات اجرا شده	۱۱۵	۵
	عدم امنیت سیستم‌های اداری الکترونیکی	۱۶۰/۵	۶		عدم وجود خط‌مشی برای امنیت اطلاعات	۹۹	۶
	پست الکترونیکی ناامن	۱۶۰/۵	۷		عدم پشتیبانی از سخت‌افزار و نرم‌افزار	۹۹	۷
	عدم توجه به تهدیدات Instant Messaging	۱۴۰	۸		عدم مشوق‌های بازدارنده	۷۴	۸
	عدم دسترسی محدود به محتوای اینترنت	۱۱۵	۹	کنترل دسترسی به اطلاعات و سیستم‌ها (رتبه ۵)	عدم مدیریت رسانه‌های قابل‌حمل مانند فلش	۲۷۴/۵	۱
	مدیریت رمزگذاری	۱۰۳/۵	۱۰		عدم کنترل رمز عبور	۱۶۰/۵	۲
	استفاده از VOIP	۷۴	۱۱		عدم امنیت در غیاب کاربر	۱۶۰/۵	۳
زیرساخت سخت‌افزار/ شبکه (رتبه ۲)	فیلتر نکردن پورت‌ها	۱۹۵	۱		عدم تأکید بر پیچیدگی رمز	۱۱۵	۴
	عدم پشتیبان از اطلاعات	۱۶۰/۵	۲		عدم تأکید بر تغییر رمز به‌صورت دوره‌ای	۱۱۵	۵
	عدم دفاع ایمنی نرم‌افزار	۱۶۰/۵	۳		عدم مدیریت دسترسی از بیرون به داخل سیستم	۹۹	۶
	عدم امکان جداسازی داده‌های حساس	۱۶۰/۵	۴		عدم احراز هویت شناسه کاربر	۹۹	۷

	عدم وجود اصالت نرم‌افزار	۱۵۳	۵		عدم کنترل و ایجاد محدودیت تردد کارکنان	۹۹	۸
	عدم وجود مولد الکترونیکی بازیابی	۱۲۶	۶		عدم شناسنامه‌دار نمودن دستگاه‌ها	۹۴/۵	۹
	عدم صدور گواهینامه برای گره‌های شبکه	۱۱۵	۷		عدم جداسازی سیستم‌های خاص	۹۰	۱۰
	عدم وجود سرور خوشه	۱۱۵	۸		عدم جداسازی شبکه‌ها	۹۰	۱۱
	عدم مجزا سازی فضای آدرس	۹۰	۹		عدم محدودیت در زمان و مدت اتصال کاربر به شبکه	۷۰/۵	۱۲
	عدم کنترل ترافیک	۹۰	۱۰		عدم ثبت‌نام کاربر	۷۰/۵	۱۳
عامل‌های انسانی (رتبه ۳)	عدم‌حمایت مدیران	۱۶۰/۵	۱		عدم به رسمیت شناختن پایانه خودکار	۵۸	۱۴
	عدم توجه به فرهنگ امنیت اطلاعات	۱۴۰	۲	توسعه سیستم اطلاعاتی امن (رتبه ۶)	شکست برای آزمون در برابر آسیب‌پذیری نرم‌افزار	۱۱۵	۱
	دخالت مدیران در تصمیمات امنیتی	۱۴۰	۳				
	عدم تشریح مسئولیت‌های امنیتی	۱۲۶	۴		عدم‌تغییر فرایند کنترل ورود به سیستم	۹۰	۲
	عدم توجه به آگاهی و آموزش امنیت اطلاعات	۱۲۶	۵				
	آگاه نبودن کارکنان از وظایف شغلی	۹۹	۶				

نتیجه‌گیری و پیشنهادها

پژوهش حاضر با هدف رتبه‌بندی ابعاد مؤثر بر امنیت اطلاعات با استفاده از رویکرد ترکیبی FMEA و تئوری خاکستری انجام شده است. برای این منظور پس از انجام مطالعات کتابخانه‌ای و استفاده از نظرات خبرگان صنعت IT شش بعد و شاخص‌های مربوط به آن‌ها مورد شناسایی قرار گرفته است. پس از انجام محاسبات مشخص گردید، بعد امنیت ارتباطات رتبه نخست را به خود اختصاص داده است. بدین معنی که امنیت ارتباطات بیشترین ریسک را برای امنیت

اطلاعات سازمان‌ها به دنبال خواهد داشت. به همین ترتیب زیرساخت سخت‌افزار، عوامل انسانی، مدیریت امنیت، کنترل دسترسی به اطلاعات و سیستم‌ها و توسعه‌ی سیستم‌های اطلاعاتی امن در رتبه‌های دوم تا ششم قرار گرفته‌اند.

در میان پژوهش‌های پیشین نزدیک‌ترین پژوهش از نظر محتوایی به تحقیق انجام شده، به دنبال رویکردی چندبعدی برای مدیریت ریسک امنیت اطلاعات با استفاده از FMEA و تئوری فازی بوده است (حبیبی، ۱۳۹۷)، رتبه‌بندی ابعاد امنیت اطلاعات به ترتیب عبارت است از : امنیت ارتباطات؛ زیرساخت؛ کنترل دسترسی به اطلاعات و سیستم‌ها؛ توسعه سیستم‌های اطلاعاتی امن و مدیریت امنیت؛ که با نتایج حاصل از پژوهش حاضر تا حد بسیاری هم‌راستا است. اگرچه شایان‌ذکر است که تحقیق حاضر بعد عوامل انسانی را نیز در نظر گرفته است. بررسی ابعاد پژوهش نشان می‌دهد که نیاز به افزایش سطح آگاهی از منظر امنیت ارتباطات و زیرساخت سخت‌افزار و شبکه از اولویت بالایی برخوردار است. علاوه بر این برای حفظ، توسعه و ارتقا سایر ابعاد مورد مطالعه ضروری است تا سرمایه‌گذاری مناسب و همراه با برنامه‌ریزی در حوزه امنیت ارتباطات و زیرساخت‌های سخت‌افزاری و شبکه انجام گیرد. از جمله فعالیت‌هایی که با توجه به شاخص‌های شناسایی موجب بهبود در این دو حوزه می‌شود عبارت است از: آموزش امنیت اطلاعات به کارکنان و افزایش سطح آگاهی آن‌ها درباره استفاده درست از گوشی‌های هوشمند و گوشی‌های دوربین‌دار، همچنین استفاده درست از سرویس‌های پیام فوری و سرویس VOIP، محدود کردن دسترسی به محتوای اینترنت از طریق فیلترینگ تخصصی و همراه با مطالعه، بهبود امنیت پست الکترونیکی با استفاده از نرم‌افزارهای تخصصی، پشتیبان گیری از اطلاعات به‌صورت دوره‌ای و یا بر اساس رویدادهای مهم پیش‌آمده. در این پژوهش مشخص گردید که عوامل انسانی جایگاه سوم را به خود اختصاص داده است که نشان‌دهنده اهمیت این بعد در به خطر انداختن امنیت اطلاعات سازمان است. امنیت اطلاعات نه‌تنها یک مسئله فنی و مدیریتی بلکه یک مسئله مربوط به رفتار کاربران است. ضروری است که همه‌ی کارکنان و شرکت‌های دیگر همکاری مطابق با این سیاست‌ها را داشته باشند. این

سیاست‌ها توسط استاندارد ISO27001 پوشش داده شده است که در آن اطلاعات نه‌تنها داده-های کامپیوتری و اطلاعات سرورها بلکه کلیه موارد حتی نگهبان سازمان یا شرکت را در نظر خواهد گرفت. در حقیقت این استاندارد یک استاندارد کسب‌وکار است که زیرساخت لازم را برای بهبود مداوم امنیت اطلاعات در سازمان فراهم می‌کند. از طرفی برای تأمین امنیت اطلاعات باید فرهنگ‌سازمانی تغییر کند و مدیران عالی سازمان می‌بایست در فرآیند تأمین امنیت اطلاعات سازمان و ایجاد این فرهنگ‌سازمانی مشارکت فعالی و مؤثری داشته باشند. همچنین تعریف سیاست‌های امنیت اطلاعات برای کم کردن آسیب‌پذیری‌های ابعاد اهمیت دارد.

با توجه به نتایج به دست آمده، به سازمان‌ها پیشنهادهای کاربردی ذیل در هر یک از ابعاد مورد مطالعه با توجه به نظرات خبرگان برای ارتقا امنیت اطلاعات ارائه می‌گردد. از جمله این اقدامات می‌توان به ایجاد دپارتمان یا تشکیلات مستقل امنیتی در سازمان، تهیه فهرستی از کلیه‌ی دارایی‌های اطلاعاتی سازمان، مشخص نمودن اهداف کنترلی در سازمان و مشخص نمودن اهداف راهبری سازمان اشاره نمود. از جمله اهداف کنترلی می‌توان به موارد زیر اشاره نمود: جلوگیری از حملات و دسترسی‌های غیرمجاز، علیه دارایی‌های اطلاعاتی سازمان، مهار خسارت‌های ناشی از ناامنی موجود در شبکه، کاهش رخنه‌پذیری به شبکه، تأمین صحت عملکرد، قابلیت دسترسی و محافظت فیزیکی برای سخت‌افزارها، متناسب با حساسیت آن‌ها، تأمین صحت عملکرد و قابلیت دسترسی برای نرم‌افزارها، متناسب با حساسیت آن‌ها، تأمین محرمانگی، صحت و قابلیت دسترسی برای اطلاعات، متناسب با طبقه‌بندی اطلاعات از حیث محرمانگی و تأمین قابلیت تشخیص هویت و حدود اختیارات کاربران. همچنین، به‌عنوان اهداف استراتژیک سازمان می‌توانند موارد زیر را در برگیرند: تأمین صحت عملکرد، قابلیت دسترسی و محافظت فیزیکی برای سخت‌افزارها، متناسب با حساسیت آن‌ها، تأمین صحت عملکرد و قابلیت دسترسی برای نرم‌افزارها، متناسب با حساسیت آن‌ها، تأمین محرمانگی، صحت و قابلیت دسترسی برای ارتباطات، متناسب با طبقه‌بندی اطلاعات از حیث محرمانگی و حساسیت ارتباطات و تأمین قابلیت تشخیص هویت، حدود اختیارات و پاسخ گوئی، حریم خصوصی.

ازآنجایی‌که امنیت ارتباطات رتبه اول را به خود اختصاص داد و بیشترین ریسک را برای سازمان به دنبال دارد پیشنهاد می‌شود اگر سازمان دارای چندین شعبه است و نیاز به ارتباط از طریق اینترنت دارند، ترجیحاً ارتباطات به‌صورت VPN یا هر روش رمزنگاری‌شده قابل‌دسترس صورت گیرد. همچنین، استفاده از سیاست برنامه‌های کاربردی بر روی یک یا چند سرور این امکان را ایجاد می‌نماید تا کاربران به‌جای نصب مجدد آن بر روی کامپیوتر خود، از برنامه‌های سرور استفاده می‌کنند. این راهکار از حیث مدیریتی و صرفه‌جویی اقتصادی از مزایای متعددی مانند عدم نیاز به خرید مجوز نرم‌افزارها، نگهداری آسان برنامه‌ها، امنیت فوق‌العاده برخوردار است. از دیگر راهکارهای پیشنهادی در این بعد می‌توان به استفاده از امضای دیجیتال با استفاده از قفل‌های سخت‌افزاری اشاره نمود. همچنین، استفاده از Proxy Server ها برای سازمان‌های کوچک‌تر و با هزینه کمتر مفید است.

از منظر زیرساخت (سخت‌افزار/شبکه) که رتبه دوم را به خود اختصاص داده است پیشنهاد می‌گردد درصورتی‌که سازمان خودکارسازی یا ابزار تحت وب دارد که نیاز به دسترسی از خارج از سازمان به آن وجود دارد، این سایت مجهز به مجوز SSL بوده و با پروتکل https منتشر شود. همچنین، کلیه اجزای شبکه و سرورها مورد نظارت قرار گرفته و خطاها و رخدادهای امنیتی و گزارش‌های آن از طریق ایمیل و SMS در اختیار مدیر شبکه قرار گیرد. ایجاد فایل‌های پشتیبان به‌صورت منظم و استفاده از UPS از دیگر پیشنهادهای در این بعد است.

از نظر عوامل انسانی که در جایگاه سوم قرار دارند برگزاری دوره آموزشی جهت تبیین خطرات ناشی از عدم توجه به مباحث امنیت اطلاعات در دو سطح برای مدیران و کارمندان سازمان پیشنهاد می‌گردد. همچنین، برگزاری دوره‌های آموزشی برای کارکنان جهت آشنایی با مباحث امنیت اطلاعات به‌صورت کاربردی و اطمینان از حفظ برنامه‌ها و آموزش امنیت اطلاعات در صورت تغییر مدیریت می‌تواند مفید واقع گردد. بعلاوه گذاشتن حداقل استاندارد-های مهارتی و دانش فنی در حوزه IT هنگام استخدام، آموزش ساخت رمزهای عبور امن و استفاده از چندین رمز برای بخش‌های مختلف، تنبیه کارکنانی که به دستورالعمل‌های امنیتی توجه نمی‌کنند، از دیگر پیشنهادهای مطرح‌شده در این بعد است.

رتبه چهارم به مدیریت امنیت اختصاص یافته است. بر همین اساس پیشنهاد می‌شود تا همواره سند خط‌مشی امنیت اطلاعات باید توسط مدیریت تائید و به تمامی کارکنان و گروه‌های ذی‌ربط برون‌سازمانی ابلاغ گردد. رویکرد اغلب سازمان‌ها در مواجه با تهدیدات، خرید محصولات امنیتی مانند فایروال و برنامه‌های ضدویروس است. به همین منظور باید همواره به این نکته توجه داشت که استفاده از گران‌قیمت‌ترین محصولات امنیتی بدون تحلیل دقیق نیازهای امنیتی، استفاده از روال‌های استاندارد در به‌کارگیری و کنترل سیستم‌های امنیتی و به روزسانی مداوم این سیستم‌ها به‌تنهایی کارساز نخواهد بود.

از منظر کنترل دسترسی به اطلاعات و سیستم‌ها سازمان‌ها باید توجه داشته باشند که برای دسترسی به هر منبع در شبکه و یا خارج از آن کاربر باید شناسایی شود و سپس تنها با توجه به نیاز منابع در اختیارش قرار بگیرد و تمام فعالیت‌های وی ثبت گردد. بستن پورت‌های ورودی/خروجی مانند درگاه فلش مموری از دیگر پیشنهادهای مهم در این بعد است. در نهایت از نظر توسعه سیستم‌های اطلاعاتی امن که رتبه ششم را به خود اختصاص داد، سازمان‌ها باید به هنگام تغییر سیستم‌عامل‌ها اقدامات لازم را جهت بازنگری برنامه‌های کاربردی مهم و حیاتی انجام دهند و آزمون‌های لازم انجام شود تا به‌این‌ترتیب از مصون ماندن عملیات سازمان در برابر تأثیرات سوء ناشی از این تغییرات اطمینان حاصل شود.

با توجه به محدودیت‌ها موجود در انجام این پژوهش و مصاحبه‌های صورت گرفته با خبرگان برای انجام پژوهش‌های آتی می‌توان پیشنهاد نمود تا رابطه اقدامات سخت و نرم سازمان‌ها بر کاهش ریسک امنیت اطلاعات سازمان‌ها مورد بررسی قرار گیرد؛ همچنین، از دیگر پیشنهادهای آتی عبارت است از اینکه آیا بررسی کنترل‌های سیاست‌های منابع انسانی در کنار اقدامات کنترلی، می‌تواند منجر به کاهش قصد تخلف و در نتیجه ایجاد سطوح بالاتری از امنیت برای اطلاعات سازمان شود یا خیر.

منابع

آرام، م. (۱۳۸۸). *بررسی و سنجش مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت گاز پارس جنوبی*. پایان‌نامه کارشناسی‌ارشد: دانشگاه شهید بهشتی.

الهی، ش. طاهری، م؛ و حسن‌زاده، ع. (۱۳۸۷). *ارائه چارچوبی برای عوامل انسانی مرتبط در امنیت سیستم‌های اطلاعاتی. پژوهش‌های مدیریت در ایران*، ۶۱، ۱-۲۲.

پورمند، ع. (۱۳۸۵). استانداردی برای مدیریت امنیت اطلاعات. *ماهنامه تدبیر*، ۱۷۵.

حریری، ن؛ و نظری، ز. (۱۳۹۱). امنیت اطلاعات در کتابخانه‌های دیجیتال ایران. *کتابداری و اطلاع‌رسانی*، ۱۶(۲)، ۹۰-۶۱.

حبیبی، ا. (۱۳۹۷). تحلیل خاکستری و تئوری خاکستری. *فصلنامه بازاریابی پارس مدیر*، ۴(۱۲)، ۲۴-۴۱.

حقیقی، ن. (۱۳۷۹). *روش‌های تجزیه تحلیل عوامل شکست و آثار آن (FMEA)*. نشر ساپکو. دوره ۲۲، شماره ۸۱، ۱۶۹-۱۲۷.

زنده‌دل نوبری، ب. *ارائه مدلی جهت رتبه‌بندی سازمان‌ها بر مبنای اندازه‌گیری و شناسایی میزان بلوغ امنیت اطلاعات در آن‌ها*. پایان‌نامه کارشناسی ارشد دانشگاه آزاد اسلامی واحد علوم تحقیقات ۱۳۸۹.

سادوسکای، ج. (۱۳۸۴). *راهنمای امنیت فناوری اطلاعات*. ترجمه میردامادی، شجاعی و صمدی. تهران: دبیرخانه شورای عالی اطلاع‌رسانی.

طاهری، م. (۱۳۸۶). *ارائه چهارچوبی برای نقش عوامل انسانی در امنیت سیستم‌های اطلاعاتی*. پایان‌نامه کارشناسی ارشد: دانشگاه تربیت مدرس.

محمودزاده، الف؛ و رجبی، م. (۱۳۸۵). مدیریت امنیت در سیستم‌های اطلاعاتی. *فصلنامه علوم مدیریت ایران*، ۱(۴)، ۷۸-۱۱۲.

مهدی، م. و وکیلی، ن. (۱۳۹۷). الگوی امکان‌سنجی و استقرار اثربخش سیستم مدیریت امنیت اطلاعات بر مبنای روش فراترکیب. *مطالعات مدیریت کسب‌وکار هوشمند*، ۷ (۲۶)، ۷۱-۹۹.

Alberts, C. J., & Dorofee, A. (2002). *Managing information security risks: the OCTAVE approach*. Addison-Wesley Longman Publishing Co., Inc.

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, 162-176.

Feng, N., & Li, M. (2011). An information systems security risk assessment model under uncertain environment. *Applied Soft Computing*, *11*(7), 4332-4340.

Feng, N., Wang, H. J., & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information sciences*, *256*, 57-73.

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & security*, *59*, 26-44.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*, 242-251.

Gusmão, A. P. H., e Silva, L. C., Silva, M. M., Poleto, T., & Costa, A. P. C. S. (2016). Information security risk analysis model using fuzzy decision theory. *International Journal of Information Management*, *36*(1), 25-34.

Kuzma, J. (2010). European digital libraries: Web security vulnerabilities. *Library Hi Tech*, *28*(3), 402-413.

Li, G. D., Yamaguchi, D., & Nagai, M. (2007). A grey-based decision-making approach to the supplier selection problem. *Mathematical and computer modelling*, *46*(3-4), 573-581.

Mahabi, V. (2010). *Information Security Awareness: System Administrators and End-User Perspectives at Florida State*

University. A Dissertation submitted to the School of Library and Information studies, Florida State University; 2010.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences*, *147*, 424-428.

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management*, *52*(1), 123-134.

Öğütçü, G., Testik, Ö. & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83-93.

Said A.R., Abdullah H., Uli J., & Mohamed Z.A. (2014). Relationship between organizational characteristics and information security knowledge management implementation. *Procedia-Social and Behavioral Sciences*, 123: 433-43.

Shamala, P., Ahmad, R., & Yusoff, M. (2013). A conceptual framework of info structure for information security risk assessment (ISRA). *Journal of Information Security and Applications*, *18*(1), 45-52.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, *57*, 14-30.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92-100.

Silva, M. M., de Gusmão, A. P. H., Poleto, T., e Silva, L. C., & Costa, A. P. C. S. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory. *International Journal of Information Management*, *34*(6), 733-740.

Vicente, E., Mateos, A., & Jiménez-Martín, A. (2014). Risk analysis in information systems: a fuzzification of the MAGERIT methodology. *Knowledge-Based Systems*, *66*, 1-12.

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & security*, *44*, 1-15.