فصلنامه علمی مطالعات مدیریت راهبردی دفاع ملی
سال هشتم، شماره 29، بهار 1403
مقاله پژوهشی، از صفحات 57-84

مقاله پژوهشی:

رویکردی جهت تجزیه و تحلیل فضای کسب و کار در راستای حکمرانی امنیت اطلاعات

فاطمه اخوان[1]، سید عبداله امین موسوی[2]، ابوالقاسم سرآبادانی[3]

تاریخ دریافت: 1401/02/18 **تاریخ پذیرش: 1401/10/19**

چکیده

داده‌ها و اطلاعات نگهداری شده در سامانه‌های فناوری اطلاعات برای کسب و کار سازمان ارزشمند و حیاتی هستند، زیرا ارزش یک کسب و کار در ارزش اطلاعات آن متمرکز است و علاوه بر ایجاد ارزش افزوده برای سازمان، خطر ازدست رفتن سرمایه و اعتبار به‌دست آمده از اعتماد مشتریان، از طرق مختلف سازمان را تهدید می‌کند و سو استفاده از رایانه و حوادث امنیتی اطلاعات نیز رو به رشد است که تاثیر مستقیم بر فرایندها و عملیات شرکت‌ها و سازمان‌ها دارد. مدیریت دارایی اطلاعات یکی از عناصر اصلی و راهبردی کسب و کار است. لذا نقش فزاینده امنیت اطلاعات در اداره سازمان‌ها و نهادها مشهود و تأمین زیرساخت‌های لازم برای تحقق این امر مهم می‌باشد. در این مقاله با استفاده از روش فراترکیب و بررسی پژوهش‌های انجام شده در این حوزه و تجزیه و تحلیل نتایج حاصله از تحقیقات کیفی، رویکردی براساس حوزه‌های تمرکز حکمرانی امنیت اطلاعات(شامل همسویی استراتژیک؛ مدیریت خطر؛ مدیریت منابع؛ اندازه‌گیری عملکرد وتحویل ارزش) ارائه شده است که به درک درست از حکمرانی امنیت اطلاعات کمک می‌کند.

کلیدواژه‌ها: فناوری اطلاعات، امنیت اطلاعات، حکمرانی فناوری اطلاعات، حکمرانی امنیت اطلاعات

1 . دانشجوی دکتری مدیریت فناوری اطلاعات، گروه مدیریت صنعتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. f63akhavan@gmail.com

2 . استادیار گروه مدیریت صنعتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران (نویسنده مسئول) saa.mousavi@iau.ac.ir

3 . استادیار گروه مدیریت فناوری اطلاعات، دانشگاه تربیت مدرس،تهران،ایران. a.sarabadani@modares.ac.ir

1. مقدمه

فناوری اطلاعات امروزه در تمام سازمان‌ها و شرکت‌ها از اهمیت بالایی برخوردار است و نحوه به‌کارگیری و مدیریت آن نیز نیازمند دارا بودن تخصص و دانش است. در واقع مدیریت فناوری اطلاعات، طراحی ساختار، تشکیلات، وظایف و مسئولیت‌ها، فرایندها و نظام‌هایی است که اجرای آنها در سازمان برای بهره‌برداری بهینه از منابع و دارایی‌های اطلاعاتی و فناوری اطلاعات، ضروری است. در اغلب سازمان‌ها و مؤسسات بزرگ، فناوری اطلاعات به‌عنوان یکی از باارزشترین دارایی‌های مجموعه به‌شمار می‌آید. سازمانی موفق است که به ارزش واقعی این دارایی پی برده و بتواند در دستیابی به منافع ذینفعان خود از آن استفاده کند. برای تحقق این مهم لازم است تدوین فرایندهای سازمانی به شکلی هدف‌مند و فرایندگرا مورد برنامه‌ریزی قرار گیرد که این خود به حکمرانی تعبیر می‌شود. با توجه به لزوم اعمال موارد فوق در حوزه فضای سایبر سازمانی، این مورد به حکمرانی سایبری و در حوزه اطلاعات به حکمرانی اطلاعات و حتی حکمرانی داده تعبیر می‌شود. از طرفی تضمین ارزش‌های فناوری اطلاعات، مدیریت مخاطرات مرتبط با آن و واپایش اطلاعات، امروزه به‌عنوان عناصر کلیدی در حکمرانی سازمانی تلقی می‌شوند. همین ارزش، ریسک و واپایش، هسته حکمرانی فناوری اطلاعات را تشکیل می‌دهند (موسسه حکمرانی فناوری اطلاعات[1]،2007)؛ (جعفر نژاد ثانی، 1392). در حال حاضر فناوری اطلاعات عضو جدا نشدنی دنیای کسب وکار است و تقریبا کسب وکاری وجود ندارد که بدون استفاده از ابزار فناوری اطلاعات به آسانی به حیات خود ادامه دهد. کسب وکارهای دنیای جدید از مزایای دنیای فناوری و ابزارهای رایانه‌ای جهت سرعت بخشیدن به کسب وکار خود و ایجاد ارزش افزوده و رونق و پیشرفت کسب وکار خود بهره می‌گیرند. داده‌ها و اطلاعات نگهداری شده در سامانه‌های فناوری اطلاعات برای کسب و کار سازمان ارزشمند و حیاتی هستند؛ زیرا ارزش یک کسب و کار در ارزش اطلاعات آن متمرکز است. افراد به دسترسی بیشتر به اطلاعات و داده‌ها پافشاری می‌کنند. همچنین، جمع‌آوری حجم عظیمی‌از داده‌ها در پایگاه داده سازمان‌ها و استفاده از ابزارهای فناوری اطلاعات، علاوه بر ایجاد ارزش افزوده برای سازمان، خطر ازدست رفتن سرمایه و اعتبار به‌دست

1. ITGI: IT Governance Institute

موسسه حکمرانی فناوری اطلاعات، توسط انجمن غیرانتفاعی ISACA در سال 1998 تأسیس شد که راهنمایی‌های لازم برای جامعه تجاری جهانی در مورد مسائل مربوط به حاکمیت دارایی‌های فناوری اطلاعات ارائه می‌کند.

آمده از اعتماد مشتریان، از طرق مختلف سازمان را تهدید می‌کند. در محیط فناورانه در حال تغییر، تهدیدات امنیت اطلاعات از سوی ویروس ها، هکرها، مجرمان و تروریست ها و همچنین تهدیدات ناشی از خطا، از دست دادن اطلاعات و سوء استفاده یا افشای اطلاعات در حال افزایش است (پریرا و سانتوس[1]، 2014)؛ (گشگری[2] و همکاران،2017)؛ (موسسه حکمرانی فناوری اطلاعات، 2006)؛ (آفتابی، 1397). پس امنیت اطلاعات یکی از مسائل چالش برانگیز سازمان ها برای انجام موفقیت‌آمیز در کسب و کار است و مدیریت آن، به دلیل فضای رقابتی کنونی، امری ضروری تلقی می شود. وجود پیچیدگی‌های فراوان در این مسئله باعث شده است با پیشرفت روزافزون فناوری اطلاعات، روز به روز به تعداد حوادث امنیتی نیز اضافه شود. از این رو، مدیران سازمان‌ها نیازمند داشتن درک درست از تعاملات و پویایی سامانه هستند تا تصمیمات مناسب برای جلوگیری از حوادث امنیتی اتخاذ کرده و موثرترین مجموعه واپایش‌ها را شناسایی، اجرا، نظارت و ارزیابی کنند تا از امنیت کافی برخوردار شوند (پریرا و سانتوس، 2014) (آفتابی، 1397). با توجه به اهمیت امنیت اطلاعات و وجود چارچوب‌ها و رویکردهای مختلف پیش رو شرکت‌ها و سازمان‌ها، در این پژوهش به ارائه رویکردی برای اجرای حکمرانی امنیت اطلاعات پرداختیم. در ابتدا به بررسی تحقیقات پیشین و نظرات محققان در زمینه شیوه‌های همسویی فناوری اطلاعات و امنیت اطلاعات با حکمرانی شرکتی و مسائل راهبردی پرداخته شد و در ادامه به تشریح مفاهیم حکمرانی فناوری اطلاعات و حکمرانی امنیت اطلاعات و رابطه میان این دو و حکمرانی شرکتی پرداخته شد. در ادامه مسئله تحقیق و روش پژوهش (که از نوع کیفی و فراترکیب است) مطرح شد. نتایج حاصل از تحقیقات، حوزه‌های تمرکز بر حکمرانی امنیت اطلاعات و در ادامه ارائه رویکردی برای اجرای حکمرانی امنیت اطلاعات است.

2. بیان مسئله

هدف حکمرانی شرکتی[3] ارائه یک راهبرد کسب و کار برای دستیابی به ماموریت، چشم‌انداز و اهداف شرکت و در عین‌حال به حداقل رساندن خطرها با استفاده از حداقل منابع است. افزایش سریع استفاده از رایانه و اینترنت و ایجاد جامعه اطلاعاتی، شرکت‌ها و سازمان‌ها را برای بهره بردن از فناوری‌های اطلاعات و نوآوری‌های آن در محیط کسب و کار مشتاق‌تر کرده است. این

1. Pereir & Santos
2. Gashgari
3. CG: Corporate Governance

خود محرکی برای سوء استفاده از رایانه و رفتارهای غیرقانونی و حوادث امنیت اطلاعات است که تاثیر مستقیم بر روندها و عملیات شرکت‌ها و سازمان‌ها دارد. با توجه به نقش فزاینده امنیت اطلاعات در اداره هر جامعه، سازمان‌ها و نهادهای دولتی و خصوصی ناگزیر به تأمین زیرساخت‌های لازم، نظارت و تشخیص زودهنگام، واکنش سریع به رویدادهای امنیتی و ایجاد اقدامات پیشگیرانه برای مدیریت امنیت اطلاعات هستند و این در حال تبدیل شدن به یک راهبرد رقابتی برای سازمان‌ها است.

به بیان ویلیامز[1] (2001) هدف امنیت اطلاعات، حفاظت از منافع کسانی است که به اطلاعات متکی هستند و همچنین حفاظت از سیستم‌ها و ارتباطاتی که اطلاعات را ارائه می‌دهند، در مقابل آسیب‌های ناشی از نقص در دسترس بودن، محرمانه بودن و یکپارچگی است.

به‌طورکلی یک برنامه امنیت اطلاعات سازمانی موثر شامل: استفاده از استانداردها، چارچوب‌ها و روش‌های بین‌المللی امنیتی که موجب جذب اعتماد ذینفعان می‌شود؛ تجزیه و تحلیل آمار و گزارش و معیارهای عملکرد اطلاعات؛ ارائه راه حل وقایع امنیت اطلاعات و حسابرسی است. امنیت اطلاعات باید در بالاترین سطوح سازمان از جمله هیئت مدیره، مدیران عالی و مدیران اجرایی مورد توجه قرار گیرد تا اطمینان حاصل شود که سازمان از تمام منابع خود به‌طور ایمن و کارآمد، با مدیریت خطر، مسئولیت‌پذیری و انطباق مناسب استفاده می‌کند و با پشتیبانی از راهبردها و اهداف سازمان، یک عملیات کسب و کار موفق و سودآور را حفظ می‌کند. حکمرانی امنیت اطلاعات که زیر مجموعه حاکمیت شرکتی است به‌عنوان چشم‌انداز امنیت اطلاعات به‌سمت یک رویکرد راهبردی و پویا حرکت می‌کند و به‌عنوان مناسب‌ترین روش نه تنها برای واپایش فرآیندهای امنیتی، بلکه برای تضمین همسویی با راهبردهای کسب و کار در نظر گرفته می‌شود. هدف مقاله تکرار جزئیات بیشتر آنچه پیش از این منتشر شده نیست، بلکه به‌عنوان راهنمای سازمان‌ها، ارائه رویکردی جهت تجزیه و تحلیل فضای کسب و کار در راستای حکمرانی امنیت اطلاعات است. در این رویکرد با دسته‌بندی معیارهای حکمرانی شرکتی (اهداف و راهبردها؛ فرآیندها؛ افراد؛ فناوری) و معیارهای امنیتی (یکپارچه‌سازی و همپوشانی استانداردها و چارچوب‌ها و بهترین روش‌های فناوری اطلاعات وامنیت اطلاعات؛ مدیریت امنیت اطلاعات؛ ابزارها و فنون؛ دستورالعمل‌های اجرایی عملی) و در ادامه انطباق با

1 Williams

حوزه‌های تمرکز حکمرانی امنیت اطلاعات که توسط موسسه حکمرانی فناوری اطلاعات تعریف و ارائه شده است. این رویکرد به هیئت حاکمه و مدیران ارشد فناوری اطلاعات و امنیت اطلاعات در درک درست و بر "چگونگی " و " آنچه" باید انجام شود، جهت دستیابی به وضعیت قابل قبول امنیت اطلاعات کمک می‌کند و تاثیر مستقیم بر تصمیم‌گیری‌ها، سیاست‌گذاری، تعیین اهداف راهبردی سازمانی و اطمینان از دستیابی آنها، مدیریت منابع و بهینه‌سازی سرمایه‌گذاری‌ها و موفقیت بلند مدت سازمان‌ها و شرکت‌ها می‌گذارد.

3.مبانی نظری و پیشینه شناسی تحقیق

در حال حاضر اطلاعات یک سرمایه اساسی و یک جنبه فزاینده قابل توجه و دارای اهمیت در کسب و کار سازمان‌ها است و کلید موفقیت در بازارهای بین‌المللی امروز برای سازمان‌ها و شرکت‌ها، ایجاد پیشرفت در مدیریت داده و اطلاعات، تجزیه و تحلیل، و یکپارچه‌سازی قوی میان برنامه‌های کاربردی سازمانی است. تقاضای فوری برای دسترسی به داده‌ها و مفید و ایمن بودن آنها وجود دارد. کسب و کار باید بتواند داده‌های خود را از تراکنش‌های مختلف جمع‌آوری کند تا به تصمیم‌گیری‌ها و جهت‌دهی مناسب در شرکت و کارآیی آنها کمک کند (آواستی[1]،2019). در سال‌های گذشته در مراحل توسعه فناوری اطلاعات و ارتباطات، ذخیره اطلاعات به‌عنوان منبع قدرت به‌شمار می‌آمد و اطلاعات فقط درگردش کار فرآیندهای شرکت‌ها رد و بدل می‌شد. با توجه به پیامدهای پیشرفت در حوزه‌های مختلف فناوری امروز و نوآوری‌های دیجیتالی آینده که موجب تغییر ماهیت عمیق رقابت، کار و اشتغال شده است، فناوری به‌تنهایی برای ارتقاء قدرت کافی نیست و رهبران باید شیوه فعالیت سازمان‌های خود را در دنیای سراسر دیجیتال و طرح جهانی‌سازی فناوری اطلاعات، بازآفرینی کنند (دیوهرست و ویلموت[2]، 2014). با توجه به اهمیت اطلاعات و احتساب آن به‌عنوان دارایی‌ها و منابع راهبردی هر سازمان، نحوه مدیریت فناوری اطلاعات و موضوع تامین امنیت اطلاعات به‌عنوان یکی از ارکان مهم برنامه‌ریزی و مسائل کلیدی سازمان‌ها به‌شمار می‌آید و تاثیر مستقیم برمدیریت هزینه‌ها و بهبود تصمیم‌گیری‌ها دارد و یکی از چالش‌های اصلی کسب و کار و اقتصاد جهانی در سازمان‌ها، کاهش حوادث امنیتی و مسئله نفوذ

1. Awasthi
2. Dewhurst & Willmott

و حفظ حریم خصوصی داده‌ها است و نیاز سازمان‌ها به اطمینان از انتقال روان و کارآمد با حفظ استانداردهای امنیتی در هر مرحله از پروژه‌های سازمانی است. این امر نه تنها برای امنیت داده‌های حیاتی درون سازمان، بلکه برای انطباق با مقررات خارجی نیز کلیدی است. بررسی‌ها نشان می دهند، پیشرفت فناورانه از بحران این مسئله نکاسته است،بلکه روز به روز به تعداد حوادث امنیتی در جهان افزوده می‌شود (دُر و الویچی[1]، 2016) (آواستی ،2019). که این امر اهمیت تامین امنیت اطلاعات را نمایان‌تر می‌کند. در دهه‌های گذشته تمرکز اصلی امنیت اطلاعات، حفاظت از سامانه های فناوری اطلاعات بود که اکثریت قریب‌به‌اتفاق اطلاعات را پردازش و ذخیره می‌کردند. این رویکرد فناوری محور است. اما امنیت اطلاعات دیدگاه بزرگتری دارد. امنیت اطلاعات، حفاظت از اطلاعات در برابر طیف گسترده‌ای از تهدیدها برای اطمینان از تداوم کسب و کار، به حداقل رساندن خطرهای کسب و کار و حداکثر کردن بازده سرمایه‌گذاری و فرصت‌های کسب و کار است؛ همچنین به‌عنوان یک اهرم توانمندساز کسب و کار، جهت جذب اعتماد ذینفعان عمل خواهد کرد و با ایجاد مزیت رقابتی یا انطباق قانونی می‌تواند ارزش‌های اضافی برای یک شرکت ایجاد کند. امنیت اطلاعات یک فرایند مستمر است که سیاست‌ها، رویه‌ها و راهبردهایی را در سازمان‌ها برای مقابله در برابر هر گونه اختلالات، تهدیدات و حملات امنیتی مانند کلاهبرداری از طریق محاسبات، جاسوسی، خرابکاری، هک رایانه، کدهای مخرب و حملات منع سرویس، آتش سوزی یا سیلاب ارائه می‌کند (کراس[2]،2018). امنیت اطلاعات علاوه بر توجه به حفاظت از اطلاعات و دانش مبتنی بر آن و صرف‌نظر از نحوه رسیدگی، پردازش، حمل و نقل یا ذخیره‌سازی آنها، به جهانی از خطرات، مزایا و فرآیندهای مرتبط با تمام منابع اطلاعاتی می‌پردازد. روشن شده است که باید با اطلاعات مانند سایر منابع حیاتی سازمانی و با همان دقت و احتیاط رفتار شود (موسسه حکمرانی فناوری اطلاعات،2008). محققان بسیاری بر این موضوع تاکید دارند که امنیت اطلاعات تنها به واپایش‌های فنی مسئله ختم نمی‌شود. عوامل مهمی‌از جمله مردم، عوامل سازمانی، فناوری، وظایف افراد، و محیط کار، در برقراری امنیت پایدار تاثیر گذارند (آفتابی، 1397). وضعیت امنیت موجود در سازمان در جنبه‌های دیگر سازمان ازجمله، مزیت رقابتی سازمان، میزان رضایت مشتری، مدیریت خطر و دیگر جنبه‌های آن تاثیر مستقیم دارد و همچنین وجود جنبه‌های

1. Dor & Elovici
2. Kraus

مختلف تاثیرگذار در این مسئله، امنیت اطلاعات را به یک زمینه چند رشته‌ای تبدیل کرده است (دُر و الویچی، 2016).

متخصصان فناوری اطلاعات و مدیران امنیت اطلاعات وظیفه تامین امنیت سازمان را بر عهده دارند؛ به‌طوریکه بر اساس اطلاعات و دانش خود از تهدیدات، اقدامات مقابله ای و واپایش‌های لازم را انتخاب می‌کنند (کیزلینگ[1] و همکاران، 2016). از وظایف مهم مدیران امنیت می‌توان به برنامه‌ریزی امنیتی؛ تعیین سیاست و الزامات امنیتی؛ مدیریت منابع انسانی؛ مدیریت خطر؛ انتخاب فناوری امنیتی؛ ارزیابی تهدید؛ پیاده‌سازی اقدامات مقابله‌ای؛ نظارت بر عملکرد سامانه؛ نگهداری و حفاظت؛ رسیدگی و پاسخگویی و حصول اطمینان از اجرای موثر و جامع چارچوب حکمرانی امنیت اطلاعات اشاره کرد (موسسه حکمرانی فناوری اطلاعات،2008)؛ (ناصره و چوی[2]،2015)؛ (آفتابی، 1397).

3.1 حکمرانی فناوری اطلاعات

اصطلاح حاکمیت یا حکمرانی فناوری اطلاعات از حکمرانی شرکتی سرچشمه می‌گیرد. حاکمیت و حکمرانی فناوری اطلاعات ارتباط تنگاتنگی با مدیریت فناوری اطلاعات دارد، اما از حیث مفاهیم، متفاوت هستند. اولین باری که از اصطلاح حکمرانی فناوری اطلاعات در ادبیات فناوری اطلاعات استفاده شد، در سال 1991 بر اساس تعریف ونکاترامان[3] بود، که حکمرانی فناوری اطلاعات را به‌عنوان وسایلی برای توصیف چگونگی واسطه‌گری روابط تجاری در کسب و کار توسط یک سامانه مبتنی بر فناوری اطلاعات توصیف کرد (سیلوا[4] و همکاران، 2019). حکمرانی فناوری اطلاعات به‌عنوان تلاش ترکیبی مدیریت اجرایی (به‌عنوان مثال مدیران عامل و مدیران ارشد اجرایی و مدیریت فناوری اطلاعات) در جهت استفاده از راهبرد فناوری اطلاعات با اهداف سازمان در ایجاد ارزش کسب و کار تعریف شده است و شامل حقوق تصمیم‌گیری و پاسخگویی است (هِیس و گرمبرگن[5]،2008)؛ (برگرون[6] و همکاران، 2017)؛ (سیلوا و همکاران، 2019)؛ (عثمان[7]،2019). به عبارت ساده، حکمرانی فناوری اطلاعات مدیران ارشد را قادر می‌سازد

1. Kiesling
2. Nazareth & Choi
.3 Venkatraman
4 Silva
5 Haes & Grembergen
6 Bergeron
7 Usman

تا کلیه فعالیت های فناوری اطلاعات در یک شرکت را هم جهت با راهبرد کسب و کار هدایت و تنظیم کنند. شرکت‌ها باید از طریق ادغام حکمرانی رسمی‌فناوری اطلاعات در ساختار کلی وظایف فناوری اطلاعات خود، به‌طور کلی با منابع فناوری اطلاعات برخورد کنند. این به آنها این امکان را می‌دهد تا اهداف، دستورالعمل‌ها و استانداردهایی را برای دستیابی به ارزش سرمایه‌گذاری در فناوری اطلاعات تعیین کنند. همچنین باید توجه کرد که تفاوت آشکاری بین حکمرانی فناوری اطلاعات و مدیریت فناوری اطلاعات وجود دارد. مدیریت فناوری اطلاعات فرایندی از سازماندهی، واپایش و نگهداری محصولات و خدمات فناوری اطلاعات است که برای عملیات موثر است در حالی که حکمرانی فناوری اطلاعات بر تحول گسترده و عملکرد فناوری اطلاعات در پاسخگویی به خواسته های کسب و کار یک سازمان و مشتریان آن در کوتاه مدت (در حال حاضر) و بلند مدت (آینده) تمرکز دارد (عثمان،2019). الگوها و استانداردهای جایگزین متعددی برای شرکت‌ها برای برنامه‌ریزی و استقرار حکمرانی فناوری اطلاعات وجود دارد که بر دستیابی به سطوح بالاتری از بلوغ و اثربخشی فناوری اطلاعات تمرکز دارد. مولفه های حکمرانی فناوری اطلاعات باید در هر رویکردی مورد توجه قرار گیرد و برای دستیابی به هماهنگی و مدیریت موثرتر فناوری اطلاعات برای شرکت ها بسیار مهم است. یک رویکرد متعادل متشکل از چارچوب بالا به پایین و نقشه راه همراه با اجرای پایین به بالا برای موفقیت ضروری است (سِلیگ[1]، 2016).

3.2 حکمرانی امنیت اطلاعات

بیشتر پژوهشگران، امنیت اطلاعات را به‌طور مستقیم با حکمرانی شرکتی مرتبط می‌دانند. ضمن اینکه محافظت از اطلاعات حساس سازمانی برای سازمان‌ها بسیار حیاتی شده است. هدف از امنیت اطلاعات محافظت از منابع ارزشمند یک سازمان، مانند اطلاعات است (هاوفه[2] و همکاران، 2016). حکمرانی امنیت اطلاعات، سامانه ای است که فعالیت امنیت اطلاعات سازمان از طریق آن هدایت و واپایش می شود (سازمان ملی استانداردایران, 1392). مولتون و کولز (2003) و پارک و همکاران (2006) حکمرانی امنیت اطلاعات را به معنای دقت کافی برای محافظت از سازمان

1. Selig
2. Haufe

می‌دانند و ایجاد و نگهداری یک محیط واپایشی برای مدیریت خطرهای مربوط به محرمانه بودن، یکپارچگی و در دسترس بودن اطلاعات و فرآیندها و سامانه‌های پشتیبانی کننده آن می‌دانند (گشگری و همکاران،2017). پوستیموس و سولمز (2004) اصطلاح حکمرانی امنیت اطلاعات را روند چگونگی پرداختن به امنیت در یک سطح اجرایی توصیف می‌کنند. ادغام امنیت اطلاعات و حکمرانی شرکتی، حکمرانی امنیت اطلاعات نامیده می‌شود. حکمرانی امنیت اطلاعات با امنیت دارایی های اطلاعاتی به شیوه‌ای جامع و شامل همه ذینفعان سازمان سروکار دارد؛ بنابراین، امنیت اطلاعات نباید فقط به‌عنوان یک موضوع فنی توسط بخش فناوری اطلاعات، بلکه باید به‌عنوان یک چالش حکمرانی در نظر گرفته شود (موسسه حکمرانی فناوری اطلاعات،2006)؛ (کارگروه سران امنیت سایبری ملی[1]، 2004)؛ (گشگری و همکاران،2017). با گذشت زمان، تعاریف در مورد عناصر مفصلی که بخشی از حکمرانی امنیت اطلاعات هستند، خاص‌تر شده و تغییر می‌کند؛ در ابتدا، تعاریف عمدتاً بر فناوری اطلاعات متمرکز بودند. حکمرانی امنیت اطلاعات می‌تواند به‌عنوان روشی کلی باشد که در آن امنیت اطلاعات به‌عنوان یک رشته برای کاهش خطرات فناوری اطلاعات به‌کار گرفته می‌شود و بر تعیین مسئولیت‌ها و روش‌های اعمال شده توسط هیئت مدیره و مدیریت اجرایی با هدف ارائه جهت‌دهی راهبردی، اطمینان از دستیابی به اهداف، اطمینان از مدیریت مناسب خطرات و تأیید استفاده مسئولانه از منابع شرکت متمرکز است. به مرور تعاریف به سمت خطرپذیری کل شرکت یا "کسب و کار" گسترش یافتند. ویلیامز و همکاران (2013) استدلال می‌کنند که معنای حکمرانی امنیت اطلاعات سیال، پویا و انعطاف‌پذیر است؛ زیرا محیط اجتماعی-فنی در حال تغییر است (شینگل و شهیم[2]،2019). حکمرانی امنیت اطلاعات نیاز به همراستا نمودن اهداف و راهبردهای امنیت اطلاعات با اهداف و راهبردهای کسب وکار و انطباق آنها با قانون، مقررات و قراردادها دارد. توصیه می‌شود این مسأله از طریق یک رویکرد مدیریت مخاطره ارزشیابی، تحلیل و پیاده‌سازی شده و به‌وسیله یک رویه واپایش داخلی پشتیبانی شود (سازمان ملی استانداردایران، 1392).

1. National Cyber Security Summit Task Force

کارگروه وظیفه حاکمیت شرکتی در دسامبر 2003 در آمریکا به منظور توسعه و ترویج یک چارچوب حاکمیتی منسجم برای اجرای برنامه‌های امنیت اطلاعات موثر تشکیل شد. و هر ساله اقدام به برگزاری نشست ملی سایبری نوآورانه‌ترین رویداد فناوری امنیت سایبری کشورآمریکا می کند.

2. Schinagl & Shahim

اداره امنیت اطلاعات بر عهده بالاترین سطوح سازمان است که باید از تمام منابع خود به‌طور ایمن و کارآمد، با مسئولیت‌پذیری و رعایت قوانین و مقررات برای حفظ عملیات موفق، حمایت از راهبرد و اهداف سازمانی و حفظ فرهنگ امنیتی استفاده کنند (موسسه حکمرانی فناوری اطلاعات، 2006) و (آلن، 2005). از آنجایی که که حکمرانی امنیت اطلاعات از رهبری، ساختار سازمانی و فرآیندها تشکیل شده است، رهبری باید مدیریت فعالانه داشته باشد و از اینکه فعالیت‌های امنیت اطلاعات در تمام سطوح سازمانی پشتیبانی، درک و اجرا می‌شود و با اهداف سازمانی همسو هستند، اطمینان حاصل نموده و آن را تضمین کند (موسسه حکمرانی فناوری اطلاعات،2006)؛ (کارگروه سران امنیت سایبری ملی، 2004)؛ (راستوگی و ون سولمز [1]، 2006)؛ (گشگری و همکاران،2017)؛ (لاو و همکاران،2010). فرآیندهای حکمرانی امنیت اطلاعات، فعالیت‌های امنیت اطلاعات هستند که از اهداف سازمانی پشتیبانی می‌کنند. این اجزای اصلی حکمرانی امنیت اطلاعات تضمین می‌کند که محرمانه بودن، یکپارچگی و در دسترس بودن دارایی‌های الکترونیکی سازمان همیشه حفظ می‌شود و اطلاعات هرگز به‌خطر نمی‌افتد (ون سولمز، 2001) و همچنین فرهنگ امنیتی را در سازمان پرورش می‌دهد و حفظ می‌کند (آلن، 2005). به‌کارگیری حکمرانی امنیت اطلاعات خوب تضمین می‌کند که راهبردهای امنیت اطلاعات با راهبرد سازمانی همسو هستند و از اهداف سازمان حمایت می‌کنند و ارزش کسب و کار را به همه ارائه می‌دهند (گشگری و همکاران،2017) و (موسسه حکمرانی فناوری اطلاعات، 2006).

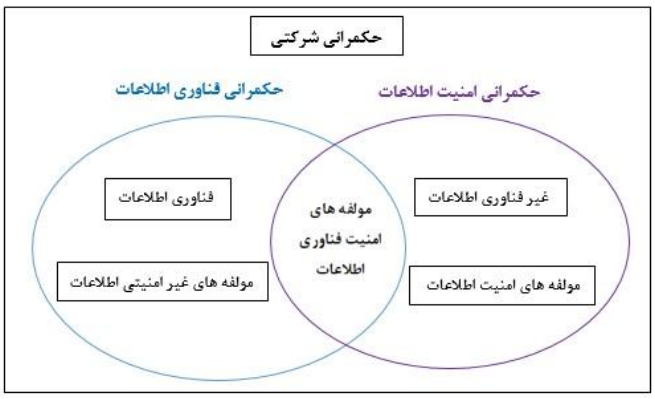
حکمرانی امنیت اطلاعات با مدیریت امنیت اطلاعات یکسان نیست؛ زیرا حکمرانی امنیت اطلاعات، مدیریت فعالیت‌های روزانه نیست؛ بلکه هدایت و واپایش سازمان و حصول اطمینان از برآورده شدن خواسته‌های سهامداران و ذینفعان (لاو [2] و همکاران،2010) و ایجاد فرهنگ سازمانی مناسب برای دستیابی به اهداف سازمان است (هاوفه و همکاران، 2016) و (دی اولیویرا [3]،2006).

3.3 رابطه بین حکمرانی امنیت اطلاعات و حکمرانی فناوری اطلاعات و حکمرانی شرکتی

چندین حوزه الگوی حکمرانی در درون سازمان وجود دارد؛ مانند حکمرانی فناوری اطلاعات،

1 Rastogi &Von Solms
2 Love
3 de Oliveira Alves

حکمرانی امنیت اطلاعات و حکمرانی سازمانی. هر الگوی حکمرانی مولفه‌های جدایی ناپذیری از حکمرانی یک سازمان است که اهمیت همراستایی با اهداف کسب وکار را نشان می دهد. برای هیأت حاکمه مفید است تا یک دید کلی‌نگر و یکپارچه از الگوی حکمرانی ایجاد کند که توصیه می شود حکمرانی امنیت اطلاعات قسمتی از آن باشد. محدوده‌های الگوی‌های حکمرانی گاهی اوقات همپوشانی دارند. در حالی که محدوده فراگیر حکمرانی فناوری اطلاعات منابع مورد نیاز جهت اکتساب، پردازش، ذخیره‌سازی و انتشار اطلاعات را در بر گرفته است؛ محدوده حکمرانی امنیت اطلاعات محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات را می پوشاند (سازمان ملی استانداردایران, 1392). اگر بخواهیم رابطه بین حکمرانی شرکتی، حکمرانی فناوری اطلاعات و حکمرانی امنیت اطلاعات را بدانیم، باید گفت حکمرانی شرکتی شامل تمام جنبه های حکمرانی برای مقابله با هر خطری است. مشابه این واقعیت که مدیران شرکتی مسئول حکمرانی شرکتی هستند، آنها همچنین مسئول حکمرانی فناوری اطلاعات و حکمرانی امنیت اطلاعات هستند. رابطه بین حکمرانی فناوری اطلاعات و حکمرانی امنیت اطلاعات به‌وضوح مشخص نشده است؛ اگرچه امنیت اطلاعات یکی از موضوعات مهم در حکمرانی فناوری اطلاعات است. حکمرانی امنیت اطلاعات نه تنها امنیت فناوری اطلاعات بلکه امنیت فیزیکی و امنیت کاغذی را نیز شامل می‌شود. رابطه بین حکمرانی امنیت اطلاعات و حکمرانی فناوری اطلاعات در شکل 1 نشان داده شده است.



شکل 1: رابطه بین حکمرانی امنیت اطلاعات و حکمرانی فناوری اطلاعات (اوکی[1] و همکاران، 2007) و

1 Ohki

(سازمان ملی استانداردایران، 1392)

4.روش‌شناسی تحقیق

پژوهش حاضر از نوع روش تحقیق فراترکیب است؛ یک رویکرد کیفی مناسب برای مطالعات در حوزه مدیریت با فراهم کردن یک نگرش نظام مند برای محققان از طریق ترکیب تحقیقات کیفی مختلف به کشف موضوعات و استعاره های جدید و اساسی می پردازد و با این روش دانش جاری را ارتقاء داده و یک دید جامع و گسترده نسبت به مسائل به‌وجود می آورد (نوبلیت و هِر[1]،1988). فراترکیب نباید با مفاهیمی چون فرامطالعه، فراتحلیل و فرانظریه اشتباه گرفته شود. فرامطالعه کلیه این مفاهیم به‌علاوه فراترکیب را دربر می گیرد. به‌طور کلی می‌توان گفت که فرامطالعه شامل چهار بخش اصلی است (دی و شومیکر[2]،2000): فراتحلیل: (تحلیل کمی‌محتوای مطالعات اولیه)؛ فراروش (تحلیل روش شناسی مطالعه اولیه)؛ فرانظریه (تحلیل نظریه های مطالعات اولیه) و فراترکیب (تحلیل کیفی محتوای رویکرد فراترکیب یک مطالعات اولیه). براساس دیدگاه زیمبر فراترکیب صرفاً بررسی ادبی متشکل از یک حوزه خاص و یا تجزیه و تحلیل ثانویه داده های اولیه از یک گروه از مطالعات تحقیقاتی نیست، بلکه تفسیری از یافته های مطالعات انتخاب شده است؛ به‌عبارت دیگر، محققانی که از فراترکیب استفاده می کنند، نه تنها سنتز یافته های یک مجموعه با دقت انتخاب شده از مطالعات را انجام می دهند، بلکه به‌طور جدی به تجزیه و تحلیل و تفسیر پیچیده و عمیق این داده‌ها می‌پردازند (زیمر[3]،2006). در فراترکیب اگرچه مطالعات زیادی مرور می شوند، اما هدف از این کار تنها انتقاد به تحقیقات انجام شده نیست، بلکه هدف آن است که افق دید افراد گسترش یافته و دانش جدیدی ایجاد شود (سندلوفسکی[4]،2007). درک این موضوع که این رویکرد صرفاً یک بررسی جامع یا خلاصه‌ای از ادبیات موجود نیست، بلکه یک سنتز و تحلیل بسیار پیچیده از تحقیقات کیفی است مهم است (اروین[5] و همکاران،2011). انجام فراترکیب مستلزم این است که محقق یک بازنگری دقیق و عمیق را در خصوص موضوع مدنظر انجام داده و یافته های تحقیقات کیفی مرتبط را با یکدیگر ترکیب کند. به

1. Noblit & Hare
2. Day & Schoemaker
3. Zimmer
4. Sandelowski
5. Erwin

این منظور از روش هفت مرحله ای سندلوسکی و باروسو شامل مراحل: 1 -تنظیم سئوال پژوهش؛ 2- مرور نظام‌مند پیشینه؛ 3 -جستجو و انتخاب مقالات مناسب؛4- استخراج اطلاعات مقالات؛ 5-تجزیه و تحلیل و ترکیب یافته‌های کیفی؛ 6 -واپایش کیفیت و 7 -ارائه یافته‌ها استفاده می‌شود (سندلوفسکی،2007).

در ابتدا براساس مسئله مورد بررسی این پژوهش به‌دنبال رویکردی مناسب برای هدایت و مشخص شدن اصول حکمرانی کسب وکار با در نظر گرفتن اصول حکمرانی امنیت اطلاعات بودیم. با توجه به اتکای روزافزون به فناوری‌ها و برای انجام کار در درون و برون سازمان‌ها، که در پی آن به جستجوی مقالات و پژوهش‌های مرتبط با موضوع طی سال‌های اخیر (جستجوی اینترنتی شامل کتب، مقالات، گزارشات و مطالعات موردی داخلی و خارجی) پرداخته شده است که منجر به مشخص شدن کلید واژه‌های اصلی و ادامه مسیر از میان 130 پژوهش گردید. در ادامه با بررسی تفسیری مقالات و غربالگری، 100 مورد از پژوهش به موضوع ارتباط بیشتری داشتند، تفکیک و این موارد نیز به دو حوزه حکمرانی کسب و کار و فناوری اطلاعات (35 مورد) و امنیت اطلاعات (65) تقسیم شده و جهت سنجش اعتبار منابع پژوهش با توجه به ماهیت تحقیق که کیفی است و برخلاف پژوهش‌های کمی‌هیچ آزمون استانداری برای روایی وجود ندارد و اغلب ماهیت پژوهش توسط پژوهشگر تعیین و تعدیل می‌شود و ماهیت مفهوم روایی در پژوهش‌های کیفی به بازنمایی مشارکت کنندگان، اهداف پژوهش و مناسب بودن فرآیندها ارتباط دارد (فقیهی و علیزاده،1384). براساس نظر کواله[1] (1996) در یک مطالعه کیفی، اعتبار (روایی) اشاره بر میزانی دارد که مشاهده محقق توانسته است پدیده مورد مطالعه یا متغیرهای مربوط به آن را انعکاس دهد. در این پژوهش، منابع با استفاده از ابزار ارزیابی مهارت‌های کیفیت CASP[2] بررسی و با استفاده از پرسشنامه مرتبط با ارزیابی پژوهش‌های کیفی که 10 سئوال ارائه می‌کند که نتایج حاصل از آن به محقق کمک می‌کند تا دقت، اعتبار و اهمیت مطالعه‌ها کیفی تحقیق را مشخص کند. این سؤالات بر موارد زیر تمرکز دارد: 1- اهداف تحقیق؛ 2- روش شناسی؛3- طرح تحقیق؛ 4 - راهبرد و روش نمونه‌برداری و انتخاب شرکت کنندگان؛ 5 – جمع‌آوری داده‌ها؛ 6-

1. Kvale
2. CASP:Critical Appraisal Skills Program
برنامه و ابزاری جهت ارزیابی مطالعات کیفی ارائه شده توسط CASPUK

جهت‌گیری محقق (رابطه بین محقق و شرکت کنندگان)؛ 7 – ملاحظات اخلاقی؛ 8 – دقت در تجزیه و تحلیل داده‌ها؛ 9– بیان واضح و روشن یافته‌ها؛ و 10– ارزش پژوهش. پاسخ به دو سئوال اول کمک شایانی به پژوهشگر جهت ادامه روند پاسخگویی و مفید بودن منبع جهت ارزیابی ارائه می‌کند. پاسخ به هر سئوال به‌صورت کیفی و سه پاسخ «بله»، «نه» یا «نمی‌توانم بگویم» است. که با معادل قرار دادن یک امتیاز کمی به هر پاسخ و جمع امتیازها، میزان اثر پژوهش در این مرحله مشخص می‌شود و موارد که زیر امتیاز میانگین مجموع امتیازات باشد، اثر بسیار کمتری دارند و فیلتر می‌شوند. در ادامه از میان منابع مرتبط‌تر اطلاعات استخراج و جمع‌بندی شد و پس از تجزیه و تحلیل اطلاعات حاصله، موارد مشابه با هم ادغام شده و در نهایت رویکرد پیشنهادی با دسته‌بندی معیارهای حکمرانی شرکتی و معیارهای امنیتی و در ادامه انطباق با 5 حوزه اصلی تمرکز حکمرانی امنیت اطلاعات و حکمرانی فناوری اطلاعات که توسط موسسه حکمرانی فناوری اطلاعات تعریف و ارائه شده است. نتایج حاصل نیز توسط دو نفر از نخبگان بررسی و ارزیابی شده است. این رویکرد به هیئت حاکمه و مدیران ارشد فناوری اطلاعات و امنیت اطلاعات در درک درست و بر "چگونگی" و "آنچه" باید انجام شود، جهت دستیابی به وضعیت قابل قبول امنیت اطلاعات کمک می‌کند و تاثیر مستقیم بر تصمیم‌گیری‌ها، سیاست‌گذاری، تعیین اهداف راهبردی سازمانی و اطمینان از دستیابی آنها، مدیریت منابع و بهینه‌سازی سرمایه‌گذاری‌ها و موفقیت بلند مدت سازمان‌ها و شرکت‌ها می‌گذارد.

5. یافته‌ها و تجزیه‌وتحلیل داده‌ها

الف: یافته‌های تحقیق

براساس پژوهش های و راهنماهای پیشین مانند تحقیقات موسسه حکمرانی فناوری اطلاعات (2008)، لوفن[1] (2019) و نیکو[2] (2018)، برای دستیابی به پیشرفت‌های قابل‌توجه، امنیت اطلاعات باید بخشی جدایی‌ناپذیر از حکمرانی سازمانی باشد و در راهبرد، مفهوم، طراحی، اجرا و عملیات ادغام شود. امنیت اطلاعات باید تقریباً در تمام راهبردهای مدیریت در نظر گرفته شود و به‌عنوان عاملی حیاتی در موفقیت شناخته شود. حکمرانی مؤثر امنیت اطلاعات مستلزم تعهد مدیریت ارشد و یک فرهنگ کلی برای امنیت اطلاعات در سطوح اجرایی و عملیاتی است.

1. Loeffen
2. Nicho

حکمرانی امنیت اطلاعات شامل عناصر مورد نیاز برای ایجاد اطمینان مدیریت ارشد است که جهت و هدف آن در وضعیت امنیتی سازمان با استفاده از یک رویکرد ساختاریافته برای اجرای یک برنامه امنیت اطلاعات منعکس می شود. هنگامی که این عناصر در جای خود قرار گرفتند، مدیریت ارشد می تواند اطمینان داشته باشد که امنیت اطلاعات کافی و موثر خواهد بود. بدیهی است که هیچ مقیاس و هدف جهانی برای امنیت اطلاعات یا حکمرانی امنیت اطلاعات وجود ندارد. از آنجایی که سنجش حکمرانی، به‌طور کلی و حکمرانی امنیت اطلاعات به‌طور خاص، دشوار است که با مجموعه ای از معیارهای عینی اندازه گیری شوند، تمایل به استفاده از معیارهایی وجود دارد که بدون توجه به ارتباط ثابت شده در دسترس هستند. برای سازمانی که هدف یا اهداف امنیت اطلاعات را مشخص کرده است، همانطور که قبلاً بحث شد، مشکل معیارها تا حدودی ساده‌تر می شود. معیارها را می توان به هر معیاری از نتایج برنامه امنیت اطلاعات که به سمت اهداف تعریف شده پیش می رود کاهش داد. با این رویکرد، راهنمایی مفید برای توسعه معیارهای خاص سازمان از سوی سازمان هایی مانند ایساکا[1]، سِرت[2]، موسسه حکمرانی فناوری اطلاعات، انجمن امنیت اطلاعات[3]، مؤسسه بین‌المللی فناوری و استانداردها[4] امکان‌پذیر است.

هدف امنیت اطلاعات، توسعه، اجرا و مدیریت یک برنامه امنیت اطلاعات است که به پنج نتیجه اساسی مشخص شده در حکمرانی امنیت اطلاعات دست یابد:

- همسویی راهبردی امنیت اطلاعات با راهبردهای کسب و کار برای حمایت از اهداف سازمانی
- مدیریت خطر موثر با اجرای اقدامات مناسب برای مدیریت و کاهش خطرات و کاهش اثرات بالقوه بر منابع اطلاعاتی تا سطح قابل قبول
- مدیریت منابع با استفاده از دانش و زیرساخت امنیت اطلاعات به طور کارآمد و مؤثر
- اندازه گیری عملکرد با اندازه گیری، نظارت و گزارش معیارهای حکمرانی امنیت اطلاعات برای اطمینان از دستیابی به اهداف سازمانی
- ایجاد ارزش با بهینه سازی سرمایه گذاری های امنیت اطلاعات در حمایت از اهداف

1. ISACA: Information Systems Audit and Control Association
2. CERT: A Computer Emergency Response Team
3. ISF: Information Security Forum
4. NIST: National Institute of Standards and Technology

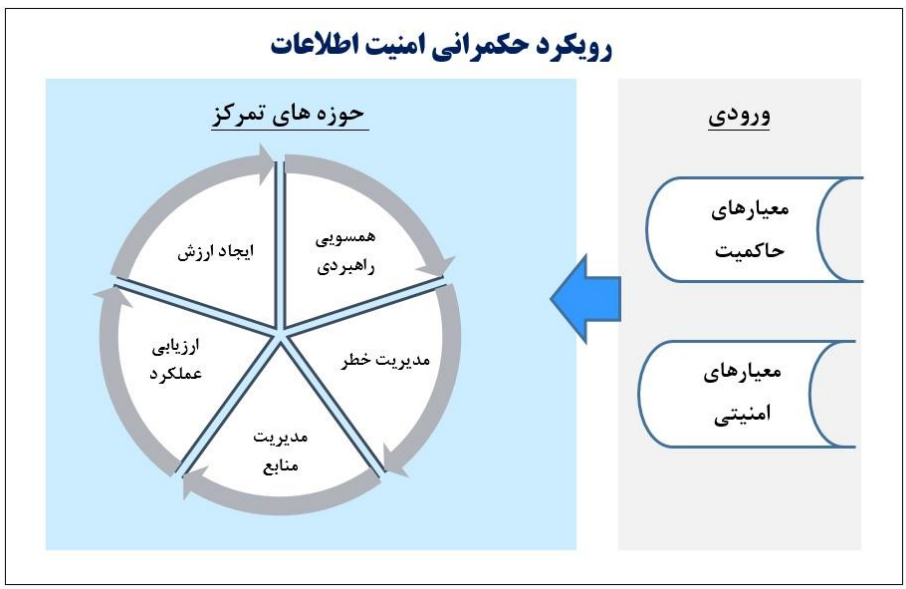
سازمانی

(لوفن ، 2019)(موسسه حکمرانی فناوری اطلاعات،2008)

ب: تجزیه و تحلیل یافته‌ها

براساس حوزه های تمرکز ارائه شده در پژوهش های مذکور که به درک درست از حکمرانی امنیت اطلاعات کمک می کند. می توان رویکردی برای حکمرانی امنیت اطلاعات ارائه کرد. شکل 2 رویکرد حکمرانی امنیت اطلاعات را نشان می‌دهد. که در ادامه به تشریح آن می‌پردازیم.

در ابتدا معیارهای حکمرانی شرکتی و معیارهای امنیتی دسته‌بندی و مشخص می شود و سپس اقدامات سازمانی را براساس 5 حوزه تمرکز حکمرانی امنیت اطلاعات همسو و منطبق می‌کنیم.



شکل 2: رویکرد حکمرانی امنیت اطلاعات

ب-1 مرحله اول

در ابتدا معیارهای حکمرانی شرکتی و معیارهای امنیتی دسته بندی و مشخص می‌شوند.

ب-1-1 معیارهای حکمرانی شرکتی:

به‌عنوان بخشی از حکمرانی شرکتی، حوزه‌های زیر برگرفته از (سایمونسون و جانسون [1]، 2006)

1. Simonsson & Johnson

در نظر گرفته خواهند شد:

• اهداف: تصمیمات راهبرد (راهبرد شرکتی الگوی تصمیم‌گیری در یک شرکت است که اهداف، مقاصد یا اهداف آن را تعیین و آشکار می‌کند؛ خط مشی‌ها و برنامه‌ها و دستورالعمل‌های اصلی و محدوده کاری امنیت اطلاعات را که شرکت باید دستیابی به آن اهداف را دنبال، واپایش و نظارت کند، مشخص می‌کند)؛

• فرآیندها: پیاده‌سازی و مدیریت فرآیندهای امنیت اطلاعات به‌همراه فعالیت‌ها و رویه‌های مربوط به آنها؛

• افراد: ساختار درون سازمانی، تعریف نقش‌ها و مسئولیت‌های ذینفعان مختلف؛

• فناوری: پیوند بین حکمرانی امنیت اطلاعات و دارایی های فیزیکی فناوری اطلاعات که سازمان مدیریت می‌کند (در داخل و خارج).

ب-1-2 معیارهای امنیتی

• یکپارچه‌سازی و همپوشانی استانداردها و چارچوب‌ها و بهترین روش‌های فناوری اطلاعات و امنیت اطلاعات منجر به نقشه‌برداری بین حوزه‌های حاکمیت فناوری اطلاعات و امنیت اطلاعات می‌شود و موجب استاندارد شدن داده‌ها و اطلاعات، تبدیل شدن به فرم‌های مفید و موثر و در حین حفظ امنیت، دسترسی کاربران به این اطلاعات است (به‌عنوان مثال خانواده ISO 270XX، ITIL و COBIT).

• مدیریت امنیت اطلاعات: سیاست ها و رویه‌های تعریف شده در سمت حکمرانی را می‌توان به بخش مدیریتی و عملیاتی امنیت اطلاعات مرتبط کرد.

• ابزارها و تکنیک ها: معمولاً چارچوب ها از ابزارهایی برای تسهیل اجرای خود استفاده می‌کنند، مانند معیارهایی برای اندازه‌گیری درجه انطباق یا الگوی‌های بلوغ برای ایجاد معیار بین سازمان‌ها.

• دستورالعمل های اجرایی عملی: رویکردهای نظری را می توان از رویکردهای عملی متمایز کرد. رویکردهای عملی شامل جزئیات فعالیت‌های اجرایی، از جمله مطالعات موردی و حتی نمونه‌های عملی است (ریبولو[1] و همکاران، 2011)

ب-2 مرحله دوم

1. Rebollo

در این مرحله اقدامات سازمانی را براساس 5 حوزه تمرکز حکمرانی امنیت اطلاعات و بر اساس توضیحات و نتایج تحقیقات مورد بررسی تحقیقات، به شرح زیر همسو و منطبق کرده‌ایم.

ب-2-1 همسویی راهبردی

همسویی راهبردی امنیت اطلاعات در حمایت از اهداف سازمانی یک هدف بسیار مطلوب است که اغلب دستیابی به آن دشوار است. باید روشن باشد که مقرون به‌صرفه بودن برنامه امنیت اطلاعات به‌طور اجتناب‌ناپذیری به‌میزان حمایت از اهداف سازمان و به چه قیمتی بستگی دارد. بدون اهداف سازمانی (به‌عنوان یک نقطه مرجع)، هر معیار دیگری، از جمله به اصطلاح «بهترین شیوه‌ها» ممکن است بیش از حد، ناکافی یا نادرست باشد. بهترین شاخص کلی فعالیت‌های امنیت اطلاعات در راستای اهداف کسب و کار (یا سازمانی)، توسعه یک راهبرد امنیت اطلاعات است که اهداف امنیت اطلاعات را در اصطلاح کسب و کار تعریف می‌کند و تضمین می‌کند که اهداف مستقیماً از برنامه ریزی از طریق اجرای سیاست‌ها، استانداردها، رویه‌ها، فرآیندها و فناوری بیان می‌شوند (موسسه حکمرانی فناوری اطلاعات،2008).

در پژوهش لوفن (2019)، اهداف اصلی همسویی راهبردی در نظر گرفتن امنیت اطلاعات به‌عنوان یک موضوع در سطح سازمان، داشتن مشارکت و رهبری قابل مشاهده و عمل بر اساس الزامات امنیت اطلاعات داخلی و خارجی است. اولین گام برای ایجاد همسویی راهبردی، پذیرش این واقعیت است که امنیت اطلاعات یک موضوع در سطح سازمان است، افراد با برنامه‌ها بر اساس فرآیندهایی کار می‌کنند. اگر امنیت اطلاعات بر روی سامانه‌هایی اجرا شوند که پشتیبانی زیرساخت‌های رابرعهده دارند درصورتیکه یکی از عناصر زنجیره به‌خوبی اجرا نشود، کل فرآیند کسب و کار متوقف می‌شود. اگرچه این امر بسیار بدیهی به‌نظر می‌رسد، اما لایه راهبردی باید به‌طور فعال نگرانی خود را برای این موضوع انجام دهد؛ زیرا پشتیبانی گسترده سازمانی از لایه راهبردی شروع می‌شود. پشتیبانی مدیریت ارشد برای امنیت اطلاعات در واقع به‌عنوان یک شاخص کلیدی موثر در موفقیت هر برنامه امنیت اطلاعات تلقی می شود. لازم است امنیت اطلاعات با کسب و کار ادغام شود. برای دستیابی به ارتباطات مناسب امنیت اطلاعات، ساختار سازمانی سازگار باید تحقق یابد. انواع مختلفی از ساختارهای سازمانی عمومی برای امنیت اطلاعات به‌طور گسترده استفاده می‌شود:

• مدیر ارشد مالی[1]: خطر ها معمولاً یک اثر مالی منفی (غیر مستقیم) دارند و بنابراین به طور معمول در بخش مالی و مدیریت خطر ترکیب می‌شوند. مشکل خطرات امنیت اطلاعات این است که ارزیابی آنها فقط با استفاده از ارزش های پولی دشوار است و این مسئولیت بخشی از کار را برعهده دارد.

• مدیر ارشد فناوری[2]: اطلاعات معمولاً صرفاً دیجیتالی تلقی می شوند و بنابراین به عنوان یک مشکل فناوری اطلاعات در نظر گرفته می شوند. اما در عمل، دیدگاه یک مدیر ارشد فناوری به امنیت فناوری محدود می شود و بنابراین نماینده کل امنیت اطلاعات نیست.

• مدیر ارشد اطلاعات[3]: بخش اطلاعات پلی بین فناوری اطلاعات و کسب و کار است و بر دستیابی به همسویی بین این دو تمرکز دارد. وقتی همسویی به‌دست آمد، کسب وکار تصمیم می‌گیرد و فناوری اطلاعات پشتیبانی می‌کند: با این حال، این امکان وجود دارد که کسب‌وکار، نحوه مدیریت امنیت اطلاعات را دیکته کند. این شیوه توصیه نمی‌شود؛ زیرا امنیت می‌تواند تأثیر منفی بر کارایی داشته باشد (که یکی از اهداف یک مدیر ارشد اطلاعات است). این ساختار منجر به نقض تفکیک وظایف می‌شود (ویتمن و ماتورد[4]، 2012).

• مدیر ارشد امنیت اطلاعات[5]: داشتن یک بخش امنیت اطلاعات در حال حاضر به این معنی است که امنیت اطلاعات بخشی از یک بخش خاص نیست، بلکه یک مشکل مشترک است. با این حال، همچنان خود را به‌عنوان یک موجودیت مجزا به‌جای دارایی همه بخش‌های دیگر می‌بینند.

• مدیر ارشد خطر[6]: مدیر ارشد خطر نقشی است که در اغلب سازمان‌های بزرگ که مدیریت خطر بخشی از کسب و کار اصلی سازمان‌ها برای مدت طولانی بوده است (مانند بانک‌ها) وجود دارد. خطرها برای این سازمان‌ها بسیار مهم و دشوارتر از آن هستند که بتوان آنها را فقط بر اساس ارزش‌های پولی ارزیابی کرد. تفاوت بین مدیر ارشد خطر و مدیر ارشد امنیت اطلاعات در این است که مدیر ارشد خطر علاوه بر خطرهای اطلاعاتی بر انواع دیگری از

1 CFO: Chief financial officer
2. CTO: Chief Technology Officer
3. CIO: Chief Information Officer
4. Whitman & Mattord
5. CISO :Chief Information Security Officer
6. CRO: Chief Risk Officer

خطرها نیز تمرکز دارد. مدیر ارشد خطر بر برنامه خطر کلی سازمان تمرکز می‌کند و بنابراین بر یک نوع خاص از خطر تمرکز نمی‌کند. مدیر ارشد خطر به‌دنبال ادغام یک برنامه خطر در سازمان است.

اینکه بهترین ساختار سازمانی چیست، بستگی به سازمان خاصی دارد که در نظر گرفته شده است. این ساختارهای مشترک بسته به سازمان می توانند نکات مثبت و منفی داشته باشند. برای مثال، یک سازمان بسیار فنی می‌تواند تا حد زیادی از امنیت تحت یک مدیر ارشد فناوری بهره‌مند شود؛ زیرا امنیت فنی نقش مهمی در کسب و کار اصلی آنها است. مستقل از ساختار انتخاب شده نیاز به یک مدیر ارشد امنیت اطلاعات است؛ زیرا امنیت اطلاعات یک فرآیند غیرمتمرکز است که در لایه‌های مختلف سازمانی گسترده شده است. امنیت اطلاعات به یک نهاد مرکزی برای هماهنگی، سازماندهی، اجرا، پیاده‌سازی، نظارت و پاسخگویی به فعالیت های امنیت اطلاعات نیاز دارد(نومینت[1]، 2019) برای دستیابی به همسویی راهبردی، نقش‌ها، مسئولیت‌ها و سیاست‌ها باید به وضوح تعریف و اجرا شوند. مدیریت راهبردی می‌تواند با تایید رسمی سیاست‌های امنیت اطلاعات و با اعلام وجود آنها حمایت خود را نشان دهد. برای بررسی اجرای این نقش‌ها، مسئولیت ها و خط مشی‌ها، انطباق باید به‌طور مرتب بررسی شود تا مطمئن شوید که سیاست‌ها هنوز مؤثر هستند و تغییرات قابل‌توجهی رخ نداده است.

به‌طور خلاصه، داشتن یک نقش در سطح مدیریت ارشد برای نظارت بر کل فرآیند امنیت اطلاعات مهم است؛ با این حال مسئولیت باید به‌طور مساوی بین کل سازمان تقسیم شود؛ این اقدام منجر به همسویی راهبردی ایجاد می‌کند و به ایجاد یک هدف مشترک کمک می‌کند. مسئولیت‌پذیری همه افراد با سیاست‌ها و رویه‌های مناسب شروع می‌شود و همه افراد باید بدانند که سیاست‌هایی وجود دارد و لازم است تا از نقش‌ها و اهداف آگاهی داشته باشند. رهبری و ایجاد حمایت سازمانی از لایه راهبردی شروع می‌شود و برای هر سازمانی که هدف آن ارتقای امنیت است، ضروری است. امنیت باید در فعالیت های کسب و کار ادغام شود و برای اطمینان از همسویی راهبردی مناسب باید مطابق با قوانین، الزامات و سیاست‌های تعیین شده کار کرد.

ب-2-2. مدیریت خطر

1. Nominet

بلکلی[1] و همکاران (2001) خطر را به عنوان "احتمال رخدادی که در صورت وقوع، ارزش کسب و کار را کاهش دهد" تعریف کردند . نحوه برخورد یک کسب و کار با رویدادهای غیرمنتظره در فرآیندهای مدیریت خطر آن تعریف میشود. مهم است که بین انواع خطر ها تمایز قائل شویم زیرا مدیریت خطر می تواند بر موارد مختلف تمرکز کند. اجرای گسترده یک فرآیند مدیریت خطر ، که به طور مداوم اطلاعات را ارائه می دهد، برای مدیریت استراتژیک اتخاذ هر تصمیم منطقی، ضروری است. نگرش یک شرکت نسبت به مدیریت خطر تا حد زیادی با استراتژی، فرهنگ، خطر پذیری و توانایی آن برای تغییر تعریف می شود .(جورج[2]، 2013). مدیریت خطر محرک اصلی حکمرانی است و به استفاده از فرصت ها و به حداقل رساندن ضرر کمک می کند. مدیریت خطر هدف نهایی تمام فعالیت های امنیت اطلاعات و در واقع تمام تلاش های تضمینی سازمانی است. یک برنامه مدیریت خطر موفق را می توان به عنوان برنامه ای تعریف کرد که به طور کارآمد، مؤثر و پیوسته انتظارات را برآورده کند و به اهداف تعریف شده دست یابد(موسسه حکمرانی فناوری اطلاعات،2008). استاندارد ISO31000 را می توان برای معرفی مدیریت خطر در سازمان استفاده کرد و سری استاندارد ISO270XX که متعلق به سازمان بین المللی استاندارد و در زمینه امنیت اطلاعات است. استاندارد ISO27001 مشخصات سیستم مدیریت امنیت اطلاعات[3] است. هدف این استاندارد تعیین الزامات ایجاد، پیاده سازی، بهره برداری، نظارت، بازبینی، نگهداری و بهبود سیستم مدیریت امنیت اطلاعات در داخل سازمان است. برای اطمینان از انتخاب کنترلهای امنیتی مناسب و متناسب جهت محافظت از دارایی های اطلاعاتی طراحی شده است. به عنوان یک روش ساختاری شناخته شده بین المللی که به مدیریت امنیت اطلاعات اختصاص دارد، دیده می شود. این استاندارد برای استفاده عمدتاً به عنوان یک چارچوب سیستم مدیریت امنیت اطلاعات در سطح بالا و نه در سطح عملیاتی طراحی شده است. استاندارد ISO27002 یک کد عملی است که کنترلهای پیشنهادی را فراهم می کند که سازمان می تواند برای رفع خطرات امنیت اطلاعات اتخاذ کند. میتوان آن را یک نقشه راه پیاده سازی یا الحاق به ISO27001 در نظر گرفت. استاندارد ISO27005 برای پر کردن خلا موجود در ISO27001 و ISO27002 از نظر مدیریت خطر امنیت اطلاعات پیشنهاد شد. البته پذیرش این

1. Blakley
2. George
3. ISMS

استاندارد به عنوان وسیله ای برای حداقل مدیریت خطر امنیت اطلاعات است.و یک استاندارد اجرایی است و توصیه هایی در مورد ارزیابی و درمان خطر دارد. استانداردی که می تواند برای تمرکز بیشتر بر روی اعمال مدیریت خطر امنیت اطلاعات و فرآیند مدیریت خطر اطلاعات مورد استفاده قرار گیرد.

مدلهای مختلف ارزیابی خطر موجود است که برخی از آنها کیفی و برخی دیگر ماهیت کمی دارند. داشتن یک هدف مشترک برای برآورد ارزش کل خطر [1] OCTAVE: ارزیابی تهدیدهای حیاتی، دارایی و آسیب پذیری، توسعه یافته توسط سِرت مدلی برای ارزیابی و برنامه ریزی استراتژیک امنیت اطلاعات مبتنی بر خطر است.جوشی و سینگ [2] (2017) به منظور بهبود سیستم سازماندهی امنیت به برخی اصول استاندارد نیاز دارند. طبقه بندی های برجسته حملات و آسیب پذیری سیستم و شبکه رایانه ای را برای بهبود طبقه بندی آسیب پذیری تجزیه و تحلیل کرده و رویکرد جدیدی را در جهت استانداردسازی شبکه و کامپیوتر پیشنهاد کرده است. یکی دیگر از مدل های برجسته ارزیابی خطر FAIR[3] تحلیل عاملی خطر اطلاعات است که چارچوبی برای درک، تجزیه و تحلیل و اندازه گیری خطر اطلاعات فراهم می کند .موسسه ملی استانداردها و چارچوب مدیریت خطر فناوری[4] مجموعه ای از فعالیتهای مربوط به مدیریت خطر سازمانی را پوشش می دهد.[5] TARA یک چارچوب ارزیابی خطر است که توسط اینتل ایجاد شده است و به شرکت ها کمک می کند تا با تقطیر اطلاعات احتمالی در مورد حملات امنیتی، خطر را مدیریت کنند. با این حال، برای اکثر سازمان ها مهم است که استاندارد با همان روشی مطابقت داشته باشد که سیستم مدیریت امنیت اطلاعات آنها با آن مطابقت دارد.

(جوشی و سینگ، 2017)(الاحمد و محمود،2012)(لوفن ،2019) (دیکسون[6]،2009)

ب-2-3 مدیریت منابع

هنگامی که سرمایه گذاری در امنیت اطلاعات انجام شده است، هوشمندانه است که از منابع استفاده کرده و آنها را در سازمان جاسازی کنیم. اختراع مجدد چرخ برای هر پروژه بی اثر خواهد

1. OCTAVE: Operationally Critical Threat, Asset and Vulnerability Evaluation
2. Joshi & Singh
3. FAIR: Factor Analysis of Information Risk
4. NIST RMF: National Institute of Standards and Technology's Risk Management Framework
5. TARA: Threat Agent Risk Assessment
6. Dixon

بود. برای استفاده مؤثر از منابع (افراد، فرآیندها، دانش و فناوری) در هر زمان، نیاز بـه جـذب و انتشار دانش در سازمان است. برای فرآیندها، می توان با استانداردسازی آنها به ایـن امـر دسـت یافت. برای اطلاعات، این را می توان با گنجاندن دانش در طرح های استاندارد پروژه بـه دسـت آورد. برای افراد، این می تواند انتشار اطلاعات در مورد منابع امنیتی باشد که از طریق کانال های ارتباطی مناسب وجود دارد. برای دستیابی به بهینه‌سازی منابع، گسترش آگـاهی در مـورد امنیـت اطلاعات، جایی که می‌توان اطلاعات را جمع‌آوری کرد، جایی که ابزارها را می‌توان یافت و غیـره مهم است. برای مثال، با تبدیل امنیت اطلاعات به بخشی از فرهنگ، کارمندان به طور خودکـار در هنگام شروع یک پروژه جدید، به دنبال دانش امنیت اطلاعات خواهند بود. زیرا بخشی از عملیات عادی آنهاست(لوفن ،2019). به طور کلی مدیریت منابع امنیت اطلاعات اصطلاحی است که برای توصیف فرآیندهای برنامه ریزی، تخصیص و کنترل منابع امنیت اطلاعات، از جمله افراد، فرآیندها و فناوری ها برای بهبود کارایی و اثربخشی راه حل های کسب و کار استفاده می شـود. (موسسـه حکمرانی فناوری اطلاعات ،2008)

ب-2-4 اندازه گیری عملکرد

امنیت برای حمایت از کسب و کار وجود دارد ، این باید یک محافظ باشد و به هیچ وجه مانع کسب و کار نشود. وقتی امنیت از کسب و کار پشتیبانی نمی کند یا حتی مـانع کسـب و کـار مـی شود، کارمندان راهی برای دور زدن کنترل های امنیتی پیدا می کنند. این مسیر جایگزین بـه یـک فرآیند سایه تبدیل می‌شود و معمولاً ناامن و مهم‌تر از آن ناشناخته است. بنابراین کنترل های امنیتی باید با همکاری تمام لایه های سازمان ایجاد شود. عملکرد برنامه امنیتـی بایـد از نظـر اثربخشـی سنجیده شود. ایجاد یک مورد کسب و کار برای کنترل های امنیتی با استفاده از معیارهای سـنتی بسیار دشوار است. با این حال، اندازه گیری ناملموس نیز مهـم اسـت، کـه بـرای انـدازه گیـری اثربخشی کامل یک برنامه امنیت اطلاعات لازم اسـت و اسـتفاده از معیارهـا در امنیـت اطلاعـات مزایای مختلفی دارد:

- به افزایش مسئولیت پذیری کمک می کنند، زیرا معیارها به تشخیص اینکه آیا کنترل های امنیتی خاص به اشتباه اجرا می شوند، اصلاً یا فقط بی اثر هستند، کمک می کنـد. یـک معیـار خاص می‌تواند پرسنل مسئول معیارهای خاص و ویژگی‌های آن را شناسایی و ردیابی کند.
- کنترل های خاص را می توان به اهداف و مقاصـد اسـتراتژیک سـازمان مـرتبط کـرد و

بنابراین برای ارزیابی اثربخشی کل برنامه امنیت اطلاعات مفید است.

- می توان از آنها برای نشان دادن انطباق با قوانین، قوانین و مقررات استفاده کرد.
- یک ورودی و بازخورد جدید و قابل سنجش برای تخصیص منابع را تشکیل می دهند. (موسسه حکمرانی فناوری اطلاعات ،2008) (لوفن ،2019)

ب-2-5 ارائه و ایجاد ارزش

ارائه ارزش جایی است که سرمایه گذاری ها و مدیریت خطر با هم برخورد می کنند. استراتژی‌ای که یک سازمان برای اجرای مدیریت خطر انتخاب می کند، نقش مهمی در تمام تصمیمات آینده دارد. مقدار مناسبی از سرمایه گذاری‌های امنیتی زمانی است که «اهداف برای امنیت محقق شود و یک موقعیت خطر قابل قبول توسط سازمان با کمترین هزینه ممکن به دست آید» . به عبارت دیگر، تحویل ارزش تابعی از همسویی استراتژیک استراتژی امنیت اطلاعات و اهداف کسب و کار است و زمانی که می توان به طور قانع کننده ای برای تمام فعالیت های امنیت اطلاعات یک مورد کسب و کاری ایجاد کرد. و سطوح سرمایه گذاری بهینه زمانی به وجود می آیند که اهداف استراتژیک برای امنیت اطلاعات محقق شود و وضعیت خطر قابل قبول با کمترین هزینه ممکن به دست آید(موسسه حکمرانی فناوری اطلاعات ،2008)(ایساکا،2018). توجه به این نکته مهم است که سرمایه گذاری ها و هزینه ها نه تنها به ارزش پولی بلکه به زمان، انرژی، هزینه های مهارت و غیره اشاره دارد. هنگامی که یک استراتژی پذیرش خطر اعمال می شود، سرمایه گذاری در مقایسه با زمانی که سازمان خطر اجتنابی را انتخاب می کند (که از منابع بیشتری طلب می کند) سنگین تر خواهد بود. هدف از ایجاد ارزش تعیین میزان فشاری است که کنترل‌های امنیت اطلاعات بر سازمان وارد می‌کنند و آیا این با استراتژی انتخاب شده مطابقت دارد یا خیر. فشار امنیت اطلاعات بر روی سازمان را می توان بر حسب ارزش مالی و همچنین بر حسب افراد، فرآیندها و سایر انواع منابع تعریف کرد.در حقیقت برای تحویل ارزش، در نظرگرفتن ارزش مالی، اندازه‌گیری قابلیت جدید خدمات و میزان اعتماد به امنیت اطلاعات (از نظر افراد و فرآیندها) مهم است(لوفن ،2019).

6.نتیجه‌گیری و پیشنهاد

سازمان‌ها باید امنیت اطلاعات را در عملکرد روزمره خود به‌طور فعال بگنجانند و به‌طور موثر با تغییرات فناورانه و خطرات فزاینده امنیت سایبری مقابله کنند. وضعیت امنیتی از سازمانی به

سازمان دیگر متفاوت است؛ اما به‌طور کلی برای هر سازمان، صرف‌نظر از فعالیت کسب و کار آنها، برقراری امنیت اطلاعات یک فعالیت بسیار پیچیده و با ماهیتی پویا است. بنابراین، مستلزم بهبود مستمر، چابکی، پاسخگویی، مسئولیت‌پذیری و انعطاف‌پذیری است.لذا توصیه می شود سازمان ها ابتدا اهداف اصلی امنیتی خود را تعیین کنند، سپس روش‌های مناسب را برای رسمی‌شدن و اعتبار بخشیدن به مدیریت خود به‌کار گیرند و در نهایت روش‌هایی را برای دستیابی به اهداف خود توسعه دهند.

به‌طور کلی حاصل ادغام امنیت اطلاعات با حکمرانی شرکتی، حکمرانی امنیت اطلاعات است و هدف امنیت اطلاعات توسعه، اجرا و مدیریت یک برنامه امنیت اطلاعات است که به پنج نتیجه اساسی مشخص شده در حکمرانی امنیت اطلاعات دست یابد:

- همسویی راهبردی امنیت اطلاعات با راهبردهای کسب و کار برای حمایت از اهداف سازمانی
- مدیریت خطر موثر با اجرای اقدامات مناسب برای مدیریت و کاهش خطرات و کاهش اثرات بالقوه بر منابع اطلاعاتی تا سطح قابل قبول
- مدیریت منابع با استفاده از دانش و زیرساخت امنیت اطلاعات به طور کارآمد و مؤثر
- اندازه گیری عملکرد با اندازه گیری، نظارت و گزارش معیارهای حکمرانی امنیت اطلاعات برای اطمینان از دستیابی به اهداف سازمانی
- ایجاد ارزش با بهینه سازی سرمایه گذاری های امنیت اطلاعات در حمایت از اهداف سازمانی

در این مقاله با استفاده از روش فراترکیب و بررسی پژوهش‌های انجام شده در این حوزه و تجزیه و تحلیل و ترکیب نتایج حاصله از تحقیقات کیفی، رویکردی براساس مشخص شدن و دسته‌بندی معیارهای حکمرانی شرکتی و معیارهای امنیتی سازمان و تلفیق و انطباق این پنج حوزه تمرکز برای حکمرانی امنیت اطلاعات ارائه شده است. این رویکرد به هیئت حاکمه و مدیران ارشد فناوری اطلاعات و امنیت اطلاعات در درک درست از حکمرانی امنیت اطلاعات کمک می‌کند و تاثیر مستقیم بر تصمیم‌گیری‌ها، سیاست گذاری، تعیین اهداف راهبردی و موفقیت بلند مدت سازمان‌ها و شرکت‌ها می‌گذارد.

فهرست منابع ومآخذ

الف. منابع فارسی

- آفتابی ، نوید (1397). یک الگوی مدیریت امنیت اطلاعات برای کاهش خطرهای احتمالی در سازمان‌های مبتنی بر فناوری اطلاعات. پایان نامه کارشناسی ارشد گرایش سامانههای اقتصادی و اجتماعی -دانشکده مهندسی صنایع دانشگاه صنعتی شریف. بازیابی از https://ganj.irandoc.ac.ir
- جعفر نژاد ثانی، سهیلا (1392). نقش پیاده‌سازی ITIL و ISMS در تداوم خدمات فناوری اطلاعات. پایان نامه کارشناسی ارشد مدیریت فن آوری اطلاعات، گرایش سامانه‌های اطلاعاتی پیشرفته -دانشکده مدیریت و حسابداری دانشگاه علامه طباطبایی. بازیابی از پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک): https://ganj.irandoc.ac.ir
- سازمان ملی استانداردایران (1392). استاندارد ایران -ایزو -آی ای سی 27014:فناوری اطلاعات – فنون امنیتی -حاکمیت امنیت اطلاعات.
- فقیهی، ابوالحسن و علیزاده، محسن (1384). روایی در تحقیق کیفی. فرهنگ مدیریت 1384 شماره 9.

ب. منابع انگلیسی

- Al-Ahmad, W., & Mohammad, B. (2012). CAN A SINGLE SECURITY FRAMEWORK ADDRESS INFORMATION SECURITY RISKS ADEQUATELY? International Journal of Digital Information and Wireless Communications (IJDIWC) 2(3), 222-230.
- Allen, J. (2005). Governing for Enterprise Security, Technical Note. Pittsburgh.
- Awasthi, A. (2019). IT Infrastructure & Enterprise Applications - Organizations Strategy and Planning. *International Journal of Science and Research (IJSR)Volume 9 Issue 4, April 2020*, 1517-1523.
- Bergeron, F., & et al. (2017). A framework for research on information technology governance in SMEs. در Strategic IT Governance and Alignment in Business Settings. doi:10.4018/978-1-5225-0861-8.ch003
- Blakley, B., & et al. (2001). Information security is information risk management. NSPW '01: Proceedings of the 2001 workshop on New security paradigms. doi:10.1145/508171.508187
- CASPUK. (2022). *https://casp-uk.net/casp-tools-checklists/*. Retrieved from www.casp-uk.net.
- Day, G. S., & Schoemaker, P. (2000). Avoiding the Pitfalls of Emerging Technologies. *California Management Review 42(2)*, 8-33. doi:10.2307/41166030
- de Oliveira Alves, G. d. (2006). Enterprise Security Governance; A practical guide to implement and control Information Security Governance (ISG).
- Dewhurst, M., & Willmott, P. (2014). Manager and machine: the new leadership equation. McKinsey Quarterly,. Retrieved from https://www.mckinsey.com/featured-insights/leadership/manager-and-machine
- Dixon, B. (2009). Understanding the FAIR risk assessment. *Nebraska CERT conference*.
- Dor, D., & Elovici, Y. (2016). A model of the information security investment decision-making process. *Computers & Security 63*, 1-13.

- Erwin, E. J., & et al. (2011). Understanding Qualitative Metasynthesis: Issues and Opportunities in Early Childhood Intervention Research. *Journal of Early Intervention 33(3)*, 186-200.
- Gashgari, G., & et al. (2017). A Proposed Best-practice Framework for Information Security. *IoTBDS 2017 - 2nd International Conference on Internet of Things, Big Data and Security* (pp. 295-301). SCITEPRESS – Science and Technology Publications, Lda.
- George, T. (2013). Risk and Compliance-For Better or Worse? ISACA Journal - 2013 Volume 4, 12-15. Retrieved from https://www.isaca.org/resources/isaca-journal/past-issues/2013/risk-and-compliance-for-better-or-worse
- Haes, S., & Grembergen, W. (2008). Analysing the Relationship Between IT Governance and Business/IT Alignment. Proceedings of the 41st Hawaii International Conference on System Sciences. Waikoloa, HI, USA: IEEE. doi:10.1109/HICSS.2008.66
- Haufe, K., & al, e. (2016). A process framework for information security management. *International Journal of Information Systems and Project Management*, 27-47. doi:10.12821/ijispm040402
- ISACA. (2018). COBIT 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY. Retrieved from www.isaca.org/COBITuse
- ITGI. (2006). Information Security Governance: Guidance for Boards of Directors and Executive Management (2nd ed.). IT Governance Institute
- ITGI. (2007). CobiT4.1. *The IT Governance Institute*. Retrieved from (www.itgi.org)
- ITGI. (2008). *Information Security Governance-Guidance for Information Security Managers*. IT Governance Institute. Retrieved from www.itgi.org
- Joshi, C., & Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in university network. Elsevier;Journal of Information Security and Applications, 128-137. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S2214212616301806?via%3Dihub
- Kiesling, E., & et al. (2016). Selecting security control portfolios: a multi-objective simulation-optimization approach. *EURO Journal on Decision* Processes Volume 4, Issues 1–2, 85-117.
- Kvale, S. (1996). Interview Views: An Introduction to Qualitative Research Interviewing. Thousand Oaks, CA: Sage Publications.
- Kraus, A. (2018). Developing an Information Security Strategy. The St. Pölten University of Applied Sciences. Retrieved from http://www.fhstp.ac.at/en
- Loeffen, F. (2019). ICT in Business-The development of an information security governance maturity model for Dutch hospitals. *Leiden Institute of Advanced Computer Science (LIACS)*.
- Love, P., & et al. (2010). GTAG Information Security Governance. *The Inistitute of Internal Auditors, 134*.
- National Cyber Security Summit Task Force (2004). Information Security Governance : a Call To Action, Coroprate Governance Report
- Nazareth, L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management Volume 52, Issue 1*, 123-134.
- Nicho, M. (2018). A Process Model for Implementing Information Systems Security Governance. Information and computer security [online], 26(1), 10-38. Retrieved from https://openair.rgu.ac.uk
- Noblit, G., & Hare, R. (1988). *Meta-ethnography: synthesizing qualitative studies*.
- Nominet. (2019). *LIFE INSIDE THE PERIMETER - Understanding the modern CISO*. NOMINET CYBER SECURITY.
- Ohki, E., & et al. (2007). Information Security Governance Framework. Information Systems

Management 24(4), 361-372. doi:10.1145/1655168.1655170

- Pereira, T., & Santos, H. (2014). Challenges in Information Security Protection. 13th European Conference on Cyber Warfare and Security (ECCWS-2014). The University of Piraeus, Piraeus, Greece.
- Rastogi, R., & von Solms, R. (2006). Information Security Governance-A Re-Definition, Security Management, Integrity, and Internal Control in Information Systems, 193, 223–236.
- Rebollo, O., & et al. (2011). Comparative Analysis of Information Security Governance Frameworks: A Public Sector. *1th European Conference on e-Coverment (ECEG'11), Ljubljani, Slovenia, 16 – 17*, (pp. 482 - 490).
- Sandelowski, M. (2007). *Handbook for Synthesizing Qualitative Research.* Springer Publishing Company.
- Schinagl, S., & Shahim, A. (2019). What do we know about information security governance?"From the basement to the boardroom":towards digital security governance. *Information & Computer Security ,Vol. 28 No.2, 2020*, 261-292. doi:10.1108/ICS-02-2019-0033
- Selig, G. (2016). IT Governance-An Integrated Framework and Roadmap: How to Plan, Deploy and Sustain for Improved Effectiveness. *Journal of International Technology and Information Management Volume 25- Issue 1*, 55-76.
- Silva, H., & et al. (2019). INFORMATION TECHNOLOGY GOVERNANCE IN SMALL AND MEDIUM. *Journal of Information Systems and Technology Management – Jistem USP-Vol. 17, 2020, e202017001*. doi:10.4301/S1807-1775202017001
- Simonsson, M., & Johnson, o. (2006). Assessment of IT Governance- A Prioritization of Cobit. *Proceedings of the Conference on Systems Engineering Research.*
- Usman, S. (2019). MIT Governance Implementation in Enterprise: A Review. *IJRECE (INTERNATIONAL JOURNAL OF RESEARCH IN ELECTRONICS AND COMPUTER ENGINEERING)VOL. 7 ISSUE 2 Apr-June 2019*, 3129-3134.
- Whitman, M. E., & Mattord, H. J. (2012). Information Security Governance for the Non-Security Business Executive. *Journal of Executive Education, 11(1) (2012)*, 97-111.
- Williams, P. (2001).Information Security Governance. Information Security Technical Report 6(3), 60–70. doi:10.1016/S13634127(01)003090
- Williams, S., & et al. (2013). Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. Electron Markets (2013) 23, 341–354. doi:10.1007/s12525-013-0137-3
- Zimmer, L. (2006). Qualitative meta-synthesis: a question of dialoguing with texts. *Journal of Advanced Nursing53(3)*, 311-318. doi:10.1111/j.1365-2648.2006.03721.x