

مقاله پژوهشی:

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

فاطمه اخوان^۱، سید عبدالله امین موسوی^۲، ابوالقاسم سرآبادانی^۳

تاریخ پذیرش: ۱۴۰۲/۱۰/۱۹

تاریخ دریافت: ۱۴۰۲/۰۲/۱۸

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 از دست رفتن سرمایه و اعتبار به دست 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 تأثیر 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 و تحویل 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

۱. دانشجوی دکتری مدیریت فناوری اطلاعات، گروه مدیریت صنعتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. f63akhavan@gmail.com
۲. استادیار گروه مدیریت صنعتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران (نویسنده مسئول) saa.mousavi@iau.ac.ir
۳. استادیار گروه مدیریت فناوری اطلاعات، دانشگاه تربیت مدرس، تهران، ایران. a.sarabadani@modares.ac.ir

۱. 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 باارزشتترین 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، ۲۰۰۷)؛ (جعفر نژاد ثانی، ۱۳۹۲). در حال حاضر فناوری اطلاعات عضو جدا نشدنی دنیای کسب و کار است و تقریباً کسب و کاری وجود ندارد که بدون استفاده از ابزار فناوری اطلاعات به آسانی به حیات خود ادامه دهد. کسب و کارهای دنیای جدید از مزایای دنیای فناوری و ابزارهای رایانه‌ای جهت سرعت بخشیدن به کسب و کار خود و ایجاد ارزش افزوده و رونق و پیشرفت کسب و کار 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 عظیمی از داده‌ها در پایگاه داده سازمان‌ها و استفاده از ابزارهای فناوری

۱. ITGI: IT Governance Institute

موسسه حکمرانی فناوری اطلاعات، توسط انجمن غیرانتفاعی ISACA در سال ۱۹۹۸ تأسیس شد که راهنمایی‌های لازم برای جامعه تجاری جهانی در مورد مسائل مربوط به حاکمیت دارایی‌های فناوری اطلاعات ارائه می‌کند.

اطلاعات، علاوه بر ایجاد ارزش افزوده برای سازمان، خطر از دست رفتن سرمایه و اعتبار به دست آمده از اعتماد مشتریان، از طرق مختلف سازمان را تهدید می کند. 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^۱، ۲۰۱۴)؛ (گشگری^۲ و همکاران، ۲۰۱۷)؛ (موسسه حکمرانی فناوری اطلاعات، ۲۰۰۶)؛ (آفتابی، ۱۳۹۷). پس امنیت اطلاعات یکی از مسائل چالش برانگیز سازمان ها برای انجام موفقیت آمیز در کسب و کار است و مدیریت آن، به دلیل فضای رقابتی کنونی، امری ضروری تلقی می شود. وجود پیچیدگی های 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 سازمان ها نیازمند داشتن درک درست از تعاملات و پویایی سامانه هستند تا تصمیمات مناسب برای جلوگیری از حوادث امنیتی اتخاذ کرده و موثرترین مجموعه واپایش ها را شناسایی، اجرا، نظارت و ارزیابی کنند تا از امنیت کافی برخوردار شوند (پریرا و سانتوس، ۲۰۱۴) (آفتابی، ۱۳۹۷). با توجه به اهمیت امنیت اطلاعات و وجود چارچوب ها و رویکردهای مختلف پیش رو شرکت ها و سازمان ها، در این پژوهش به ارائه رویکردی برای اجرای حکمرانی امنیت اطلاعات پرداختیم. در ابتدا به بررسی تحقیقات پیشین و نظرات محققان در زمینه شیوه های 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، حوزه های تمرکز بر حکمرانی امنیت اطلاعات و در ادامه ارائه رویکردی برای اجرای حکمرانی امنیت اطلاعات است.

۲. بیان مسئله

هدف حکمرانی شرکتی^۳ ارائه یک راهبرد کسب و کار برای دستیابی به مأموریت، چشم انداز و اهداف شرکت و در عین حال به حداقل رساندن خطرها با استفاده از حداقل منابع است. افزایش

۱. Pereir & Santos

۲. Gashgari

۳. CG: Corporate Governance

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 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^۱ (۲۰۰۱) 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

۱ Williams

همپوشانی استانداردها و چارچوب‌ها و بهترین روش‌های فناوری اطلاعات و امنیت اطلاعات؛ مدیریت امنیت اطلاعات؛ ابزارها و فنون؛ دستورالعمل‌های اجرایی عملی) و در ادامه انطباق با 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.

۳. 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^۱، ۲۰۱۹). در سال‌های گذشته در مراحل توسعه فناوری اطلاعات و ارتباطات، ذخیره اطلاعات به‌عنوان منبع قدرت به‌شمار می‌آمد و اطلاعات فقط در گردش 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^۲، ۲۰۱۴). 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

۱. Awasthi

۲. Dewhurst & Willmott

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 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 می‌دهند، پیشرفت فناوریانه از بحران این مسئله نکاسته است، بلکه روز به روز به تعداد حوادث امنیتی در جهان افزوده می‌شود (دُر و الویچی^۱، ۲۰۱۶) (آواستی، ۲۰۱۹). که این امر اهمیت تامین امنیت اطلاعات را نمایان تر می‌کند. در دهه‌های گذشته تمرکز اصلی امنیت اطلاعات، حفاظت از سامانه‌های فناوری اطلاعات بود که اکثریت قریب به اتفاق 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^۲، ۲۰۱۸). 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، ۲۰۰۸). محققان بسیاری بر این موضوع تاکید دارند که امنیت اطلاعات تنها به واپایش‌های فنی مسئله ختم نمی‌شود. عوامل مهمی از جمله مردم، عوامل سازمانی، فناوری، وظایف افراد، و محیط کار، در برقراری امنیت پایدار تاثیر گذارند (آفتابی، ۱۳۹۷).

۱. Dor & Elovici

۲. Kraus

وضعیت امنیت موجود در سازمان در جنبه های دیگر سازمان از جمله، مزیت رقابتی سازمان، میزان رضایت مشتری، مدیریت خطر و دیگر جنبه های آن تاثیر مستقیم دارد و همچنین وجود جنبه های مختلف تاثیرگذار در این مسئله، امنیت اطلاعات را به یک زمینه چند رشته ای تبدیل کرده است (دُر و الویچی، ۲۰۱۶).

متخصصان فناوری اطلاعات و مدیران امنیت اطلاعات وظیفه تامین امنیت سازمان را بر عهده دارند؛ به طوریکه بر اساس اطلاعات و دانش خود از تهدیدات، اقدامات مقابله ای و واپایش های لازم را انتخاب می کنند (کیزلینگ^۱ و همکاران، ۲۰۱۶). از وظایف مهم مدیران امنیت می توان به برنامه ریزی امنیتی؛ تعیین سیاست و الزامات امنیتی؛ مدیریت منابع انسانی؛ مدیریت خطر؛ انتخاب فناوری امنیتی؛ ارزیابی تهدید؛ پیاده سازی اقدامات مقابله ای؛ 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، ۲۰۰۸)؛ (ناصره و چوی^۲، ۲۰۱۵)؛ (آفتابی، ۱۳۹۷).

۳،۱ حکمرانی فناوری اطلاعات

اصطلاح حاکمیت یا حکمرانی فناوری اطلاعات از حکمرانی شرکتی سرچشمه می گیرد. 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 ۱۹۹۱ بر اساس تعریف ونکاترامان^۳ بود، که حکمرانی فناوری اطلاعات را به عنوان وسایلی برای توصیف چگونگی واسطه گری روابط تجاری در کسب و کار توسط یک سامانه مبتنی بر فناوری اطلاعات توصیف کرد (سیلوا^۴ و همکاران، ۲۰۱۹). حکمرانی فناوری اطلاعات به عنوان تلاش ترکیبی مدیریت اجرایی (به عنوان 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 تصمیم گیری و

۱. Kiesling

۲. Nazareth & Choi

۳. Venkatraman

۴. Silva

پاسخگویی است (هیس و گرمبرگن^۱، ۲۰۰۸)؛ (برگرون^۲ و همکاران، ۲۰۱۷)؛ (سیلوا و همکاران، ۲۰۱۹)؛ (عثمان^۳، ۲۰۱۹). به عبارت ساده، حکمرانی فناوری اطلاعات مدیران ارشد را قادر می‌سازد تا کلیه فعالیت‌های فناوری اطلاعات در یک شرکت را هم جهت با راهبرد کسب و کار هدایت و تنظیم کنند. شرکت‌ها باید از طریق ادغام حکمرانی رسمی فناوری 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 خواسته‌های کسب و کار یک سازمان و مشتریان آن در کوتاه مدت (در حال حاضر) و بلند مدت (آینده) تمرکز دارد (عثمان، ۲۰۱۹). 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. مولفه‌های حکمرانی فناوری اطلاعات باید در هر رویکردی مورد توجه قرار گیرد و برای دستیابی به هماهنگی و مدیریت موثرتر فناوری اطلاعات برای شرکت‌ها 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 (سلیگ^۴، ۲۰۱۶).

۳,۲ 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

۱ Haes & Grembergen

۲ Bergeron

۳ Usman

۴. Selig

امنیت اطلاعات محافظت از منابع ارزشمند یک سازمان، مانند اطلاعات است (هاوفه^۱ و همکاران، ۲۰۱۶). حکمرانی امنیت اطلاعات، سامانه ای است که فعالیت امنیت اطلاعات سازمان از طریق آن هدایت و واپایش می شود (سازمان ملی استاندارد ایران، ۱۳۹۲). مولتون و کولز (۲۰۰۳) و پارک و همکاران (۲۰۰۶) حکمرانی امنیت اطلاعات را به معنای دقت کافی برای محافظت از سازمان می دانند و ایجاد و نگهداری یک محیط واپایشی برای مدیریت خطرهای مربوط به محرمانه بودن، یکپارچگی و در دسترس بودن اطلاعات و فرایندها و سامانه‌های پشتیبانی کننده آن می‌دانند (گشگری و همکاران، ۲۰۱۷). پوستیموس و سولمز (۲۰۰۴) 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، ۲۰۰۶)؛ (کارگروه سران امنیت سایبری ملی^۲، ۲۰۰۴)؛ (گشگری و همکاران، ۲۰۱۷). با گذشت زمان، تعاریف در مورد عناصر مفصلی که بخشی از حکمرانی امنیت اطلاعات هستند، خاص تر 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 (۲۰۱۳) استدلال می‌کنند که معنای حکمرانی امنیت اطلاعات سیال، پویا و انعطاف‌پذیر است؛ زیرا محیط

۱. Haufe

۲. National Cyber Security Summit Task Force

کارگروه وظیفه حاکمیت شرکتی در دسامبر ۲۰۰۳ 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 کشور آمریکا می‌کند.

اجتماعی- فنی در حال تغییر است (شینگل و شهیم^۱، ۲۰۱۹). حکمرانی امنیت اطلاعات نیاز به همراستا نمودن اهداف و راهبردهای امنیت اطلاعات با اهداف و راهبردهای کسب و کار و انطباق آنها با قانون، مقررات و قراردادهای 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 استاندارد ایران، ۱۳۹۲).

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، ۲۰۰۶) و (آلن، ۲۰۰۵). 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، ۲۰۰۶)؛ (کارگروه سران امنیت سایبری ملی، ۲۰۰۴)؛ (راستوگی و ون سولمز^۲، ۲۰۰۶)؛ (گشگری و همکاران، ۲۰۱۷)؛ (لاو و همکاران، ۲۰۱۰). 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، ۲۰۰۱) و همچنین فرهنگ امنیتی را در سازمان پرورش می‌دهد و حفظ می‌کند (آلن، ۲۰۰۵). 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، ۲۰۱۷) و (موسسه حکمرانی فناوری اطلاعات، ۲۰۰۶).

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

۱. Schinagl & Shahim

۲ Rastogi & Von Solms

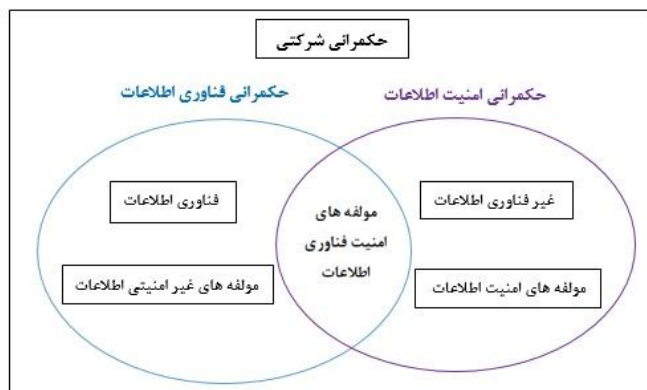
برآورده شدن خواسته‌های سهامداران و ذینفعان (لاو^۱ و همکاران، ۲۰۱۰) و ایجاد فرهنگ سازمانی مناسب برای دستیابی به اهداف سازمان است (هاوفه و همکاران، ۲۰۱۶) و (دی اولیویرا، ۲۰۰۶).

۳,۳ 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، حکمرانی امنیت اطلاعات و حکمرانی سازمانی. هر الگوی حکمرانی مولفه‌های جدایی ناپذیری از حکمرانی یک سازمان است که اهمیت همراستایی با اهداف کسب و کار را نشان می‌دهد. برای هیأت حاکمه مفید است تا یک دید کلی‌نگر و یکپارچه از الگوی حکمرانی ایجاد کند که توصیه می‌شود 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 می‌پوشاند (سازمان ملی استاندارد ایران، ۱۳۹۲). اگر بخواهیم رابطه بین حکمرانی شرکتی، حکمرانی فناوری اطلاعات و حکمرانی امنیت اطلاعات را بدانیم، باید گفت حکمرانی شرکتی شامل تمام جنبه‌های 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 ۱ نشان داده شده است.

۱ Love

۲ de Oliveira Alves



شکل ۱: رابطه بین حکمرانی امنیت اطلاعات و حکمرانی فناوری اطلاعات (اوکی^۱ و همکاران، ۲۰۰۷) و

(سازمان ملی استاندارد ایران، ۱۳۹۲)

۴. 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 استعاره‌های جدید و اساسی می‌پردازد و با این روش دانش جاری را ارتقاء داده و یک دید جامع و گسترده نسبت به مسائل به‌وجود می‌آورد (نوبلیت و هر^۲، ۱۹۸۸). فراترکیب نباید با مفاهیمی چون فرامطالعه، فراتحلیل و فرانظریه اشتباه گرفته شود. فرامطالعه کلیه این مفاهیم به‌علاوه فراترکیب را دربر می‌گیرد. به‌طور کلی می‌توان گفت که فرامطالعه شامل چهار بخش اصلی است (دی و شومیکر^۳، ۲۰۰۰): فراتحلیل: (تحلیل کمی محتوای مطالعات اولیه)؛ فراروش (تحلیل روش‌شناسی مطالعه اولیه)؛ فرانظریه (تحلیل نظریه‌های مطالعات اولیه) و فراترکیب (تحلیل کیفی محتوای رویکرد فراترکیب یک مطالعات اولیه). براساس دیدگاه زیمر فراترکیب صرفاً بررسی ادبی متشکل از یک حوزه خاص و یا تجزیه و تحلیل ثانویه داده‌های اولیه از یک گروه از مطالعات تحقیقاتی نیست، بلکه تفسیری از یافته‌های مطالعات

۱ Ohki

۲. Noblit & Hare

۳. Day & Schoemaker

انتخاب شده است؛ به عبارت 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 به طور جدی به تجزیه و تحلیل و تفسیر پیچیده و عمیق این داده ها می پردازند (زیمرا^۱، ۲۰۰۶). 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^۲، ۲۰۰۷). درک این موضوع که این رویکرد صرفاً یک بررسی جامع یا خلاصه ای از ادبیات موجود نیست، بلکه یک سنتز و تحلیل بسیار پیچیده از تحقیقات کیفی است مهم است (اروین^۳ و همکاران، ۲۰۱۱). 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 این منظور از روش هفت مرحله ای سندلوفسکی و باروسو شامل مراحل: ۱-تنظیم سئوال پژوهش؛ ۲- مرور نظام مند پیشینه؛ ۳- جستجو و انتخاب مقالات مناسب؛ ۴- استخراج اطلاعات مقالات؛ ۵- تجزیه و تحلیل و ترکیب یافته های کیفی؛ ۶- واپایش کیفیت و ۷- ارائه یافته ها استفاده می شود (سندلوفسکی، ۲۰۰۷).

در ابتدا براساس مسئله مورد بررسی این پژوهش به دنبال رویکردی مناسب برای هدایت و مشخص شدن اصول حکمرانی کسب و کار با در نظر گرفتن اصول حکمرانی امنیت اطلاعات بودیم. با توجه به اتکای روزافزون به فناوری ها و برای انجام کار در درون و برون سازمان ها، که در پی آن به جستجوی مقالات و پژوهش های مرتبط با موضوع طی سال های اخیر (جستجوی اینترنتی شامل کتب، مقالات، گزارشات و مطالعات موردی داخلی و خارجی) پرداخته شده است که منجر به مشخص شدن کلید واژه های اصلی و ادامه مسیر از میان ۱۳۰ پژوهش گردید. در ادامه با بررسی تفسیری مقالات و غربالگری، ۱۰۰ مورد از پژوهش به موضوع ارتباط بیشتری داشتند، تفکیک و این موارد نیز به دو حوزه حکمرانی کسب و کار و فناوری اطلاعات (۳۵ مورد) و امنیت اطلاعات (۶۵) تقسیم شده و جهت سنجش اعتبار منابع پژوهش با توجه به ماهیت تحقیق که کیفی است و برخلاف پژوهش های کمی هیچ آزمون استناداری برای روایی وجود ندارد و اغلب

۱. Zimmer

۲. Sandelowski

۳. Erwin

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، ۱۳۸۴). براساس نظر کواله^۱ (۱۹۹۶) 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^۲ CASP بررسی و با استفاده از پرسشنامه مرتبط با ارزیابی پژوهش‌های کیفی که ۱۰ سؤال 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: ۱- اهداف تحقیق؛ ۲- روش شناسی؛ ۳- طرح تحقیق؛ ۴- راهبرد و روش نمونه‌برداری و انتخاب شرکت کنندگان؛ ۵- جمع‌آوری داده‌ها؛ ۶- جهت‌گیری محقق (رابطه بین محقق و شرکت کنندگان)؛ ۷- ملاحظات اخلاقی؛ ۸- دقت در تجزیه و تحلیل داده‌ها؛ ۹- بیان واضح و روشن یافته‌ها؛ و ۱۰- ارزش پژوهش. پاسخ به دو سؤال اول کمک شایانی به پژوهشگر جهت ادامه روند پاسخگویی و مفید بودن منبع جهت ارزیابی ارائه می‌کند. پاسخ به هر سؤال به صورت 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 مرتبط تر 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 ۵ 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

۱. Kvale

۲. CASP: Critical Appraisal Skills Program

برنامه و ابزاری جهت ارزیابی مطالعات کیفی ارائه شده توسط CASPUK

اطمینان از دستیابی آنها، مدیریت منابع و بهینه‌سازی سرمایه‌گذاری‌ها و موفقیت بلند مدت سازمان‌ها و شرکت‌ها می‌گذارد.

۵. یافته‌ها و تجزیه و تحلیل داده‌ها

الف: یافته‌های تحقیق

براساس پژوهش‌های و راهنماهای پیشین مانند تحقیقات موسسه حکمرانی فناوری اطلاعات (۲۰۰۸)، لوفن^۱ (۲۰۱۹) و نیکو^۲ (۲۰۱۸)، برای دستیابی به پیشرفت‌های قابل توجه، 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. 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 می‌شود. هنگامی که این عناصر در جای خود قرار گرفتند، مدیریت ارشد می‌تواند اطمینان داشته باشد که امنیت اطلاعات کافی و مؤثر 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 مجموعه‌ای از معیارهای عینی اندازه‌گیری 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 می‌شود. معیارها را می‌توان به هر معیاری از نتایج برنامه امنیت اطلاعات که به سمت اهداف تعریف شده پیش می‌رود کاهش داد. با این رویکرد، راهنمایی مفید برای توسعه معیارهای خاص سازمان از سوی سازمان‌هایی مانند ایساکا^۳، سیرت^۴، موسسه حکمرانی فناوری اطلاعات، انجمن

۱. Loeffen

۲. Nicho

۳. ISACA: Information Systems Audit and Control Association

۴. CERT: A Computer Emergency Response Team

امنیت اطلاعات^۱، مؤسسه بین‌المللی فناوری و استانداردها^۲ 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
- اندازه‌گیری عملکرد با اندازه‌گیری، نظارت و گزارش معیارهای حکمرانی امنیت اطلاعات برای اطمینان از دستیابی به اهداف سازمانی
- ایجاد ارزش با بهینه‌سازی سرمایه‌گذاری‌های امنیت اطلاعات در حمایت از اهداف سازمانی

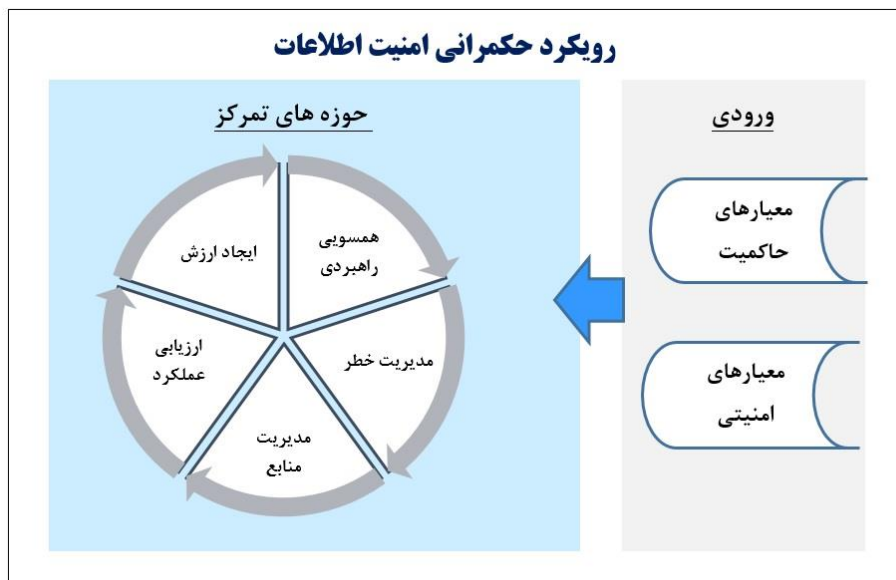
(لوفن، ۲۰۱۹) (موسسه حکمرانی فناوری اطلاعات، ۲۰۰۸)

ب: تجزیه و تحلیل یافته‌ها

براساس حوزه‌های تمرکز ارائه شده در پژوهش‌های مذکور که به درک درست از حکمرانی امنیت اطلاعات کمک می‌کند. می‌توان رویکردی برای حکمرانی امنیت اطلاعات ارائه کرد. شکل ۲ 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 می‌شود و سپس اقدامات سازمانی را براساس ۵ حوزه تمرکز حکمرانی امنیت اطلاعات همسو و منطبق می‌کنیم.

۱. ISF: Information Security Forum

۲. NIST: National Institute of Standards and Technology



شکل ۲: رویکرد حکمرانی امنیت اطلاعات

ب-۱ مرحله اول

در ابتدا معیارهای حکمرانی شرکتی و معیارهای امنیتی دسته بندی و مشخص می شوند.

ب-۱-۱ معیارهای حکمرانی شرکتی:

به عنوان بخشی از حکمرانی شرکتی، حوزه های زیر برگرفته از (سایمونسون و جانسون^۱، ۲۰۰۶) در نظر گرفته خواهند شد:

- اهداف: تصمیمات راهبرد (راهبرد شرکتی الگوی تصمیم گیری در یک شرکت است که اهداف، مقاصد یا اهداف آن را تعیین و آشکار می کند؛ خط مشی ها و برنامه ها و دستورالعمل های اصلی و محدوده کاری امنیت اطلاعات را که شرکت باید دستیابی به آن اهداف را دنبال، واپایش و نظارت کند، مشخص می کند)؛
- فرآیندها: پیاده سازی و مدیریت فرآیندهای امنیت اطلاعات به همراه فعالیت ها و رویه های مربوط به آنها؛
- افراد: ساختار درون سازمانی، تعریف نقش ها و مسئولیت های ذینفعان مختلف؛

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

ب-۱-۲ 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 ۲۷۰XX، ITIL و COBIT).

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

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

• دستورالعمل‌های اجرایی عملی: رویکردهای نظری را می‌توان از رویکردهای عملی متمایز کرد. رویکردهای عملی شامل جزئیات فعالیت‌های اجرایی، از جمله مطالعات موردی و حتی نمونه‌های عملی است (ریبولو^۱ و همکاران، ۲۰۱۱).

ب-۲ مرحله دوم

در این مرحله اقدامات سازمانی را براساس ۵ حوزه تمرکز حکمرانی امنیت اطلاعات و بر اساس توضیحات و نتایج تحقیقات مورد بررسی تحقیقات، به شرح زیر همسو و منطبق کرده‌ایم.

ب-۲-۱ 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 برنامه‌ریزی از طریق اجرای سیاست‌ها، استانداردها، رویه‌ها، فرآیندها و فناوری بیان می‌شوند (موسسه حکمرانی فناوری اطلاعات، ۲۰۰۸).

در پژوهش لوفن (۲۰۱۹)، اهداف اصلی همسویی راهبردی در نظر گرفتن امنیت اطلاعات به عنوان 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 رابرهده دارند در صورتیکه یکی از عناصر زنجیره به‌خوبی اجرا نشود، کل فرآیند کسب و کار متوقف می‌شود. اگرچه این امر بسیار بدیهی به نظر 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 می‌شود. 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^۱: خطرهای معمولاً یک اثر مالی منفی (غیر مستقیم) دارند و بنابراین به‌طور معمول در بخش مالی و مدیریت خطر ترکیب می‌شوند. مشکل خطرات امنیت اطلاعات این است که ارزیابی آنها فقط با استفاده از ارزش‌های پولی دشوار است و این مسئولیت بخشی از کار را برعهده دارد.
- مدیر ارشد فناوری^۲: اطلاعات معمولاً صرفاً دیجیتالی تلقی می‌شوند و بنابراین به‌عنوان یک مشکل فناوری اطلاعات در نظر گرفته می‌شوند. اما در عمل، دیدگاه یک مدیر ارشد فناوری به امنیت فناوری محدود می‌شود و بنابراین نماینده کل امنیت اطلاعات نیست.

۱ CFO: Chief financial officer

۲ CTO: Chief Technology Officer

• مدیر ارشد اطلاعات^۱: بخش اطلاعات پلی بین فناوری اطلاعات و کسب و کار است و بر دستیابی به همسویی بین این دو تمرکز دارد. وقتی همسویی به دست آمد، کسب و کار تصمیم می‌گیرد و فناوری اطلاعات پشتیبانی می‌کند: با این حال، این امکان وجود دارد که کسب و کار، 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^۲، ۲۰۱۲).

• مدیر ارشد امنیت اطلاعات^۳: 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 به عنوان یک موجودیت مجزا به جای دارایی همه بخش‌های دیگر می‌بیند.

• مدیر ارشد خطر^۴: 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 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 به دنبال 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 می‌توانند 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

۱. CIO: Chief Information Officer

۲. Whitman & Mattord

۳. CISO: Chief Information Security Officer

۴. CRO: Chief Risk Officer

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 فعالیت‌های امنیت اطلاعات نیاز دارد (نومینت^۱، ۲۰۱۹) 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، مسئولیت‌ها و خط‌مشی‌ها، 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 فعالیت‌های کسب و کار ادغام شود و برای اطمینان از همسویی راهبردی مناسب باید مطابق با قوانین، الزامات و سیاست‌های تعیین شده کار کرد.

ب-۲-۲. مدیریت خطر

بلکلی^۲ و همکاران (۲۰۰۱) 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 خطرها تمایز قائل شویم زیرا مدیریت خطر می‌تواند بر موارد مختلف تمرکز کند. اجرای گسترده یک فرآیند مدیریت خطر، که به‌طور مداوم اطلاعات را ارائه می‌دهد، برای مدیریت استراتژیک اتخاذ هر تصمیم منطقی، ضروری است. نگرش یک شرکت نسبت به مدیریت خطر تا حد زیادی با

۱. Nominet

۲. Blakley

استراتژی، فرهنگ، خطر پذیری و توانایی آن برای تغییر تعریف می شود. (جورج^۱، ۲۰۱۳). 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، ۲۰۰۸). استاندارد ISO ۳۱۰۰۰ را می توان برای معرفی مدیریت خطر در سازمان استفاده کرد و سری استاندارد ISO ۲۷۰XX که متعلق به سازمان بین المللی استاندارد و در زمینه امنیت اطلاعات است. استاندارد ISO ۲۷۰۰۱ مشخصات سیستم مدیریت امنیت اطلاعات^۲ 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 کنترل های 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 ISO ۲۷۰۰۲ یک کد عملی است که کنترل های 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 ISO ۲۷۰۰۱ در نظر گرفت. استاندارد ISO ۲۷۰۰۵ برای پر کردن خلا موجود در ISO ۲۷۰۰۱ و ISO ۲۷۰۰۲ از نظر مدیریت خطر امنیت اطلاعات پیشنهاد شد. البته پذیرش این 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. استاندارد 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

۱. George

۲. ISMS

دارند. داشتن یک هدف مشترک برای برآورد ارزش کل خطر^۱ OCTAVE: ارزیابی تهدیدهای حیاتی، دارایی و آسیب پذیری، توسعه یافته توسط سیرت مدلی برای ارزیابی و برنامه ریزی استراتژیک امنیت اطلاعات مبتنی بر خطر است. جوشی و سینگ^۲ (۲۰۱۷) 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^۳ FAIR 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^۴ مجموعه ای از فعالیتهای مربوط به مدیریت خطر سازمانی را پوشش می دهد.^۵ TARA یک چارچوب ارزیابی خطر است که توسط ایستل 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، ۲۰۱۷) (الاحمد و محمود، ۲۰۱۲) (لوفن، ۲۰۱۹) (دیکسون، ۲۰۰۹)

ب-۲-۳ 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 بود. برای استفاده مؤثر از منابع (افراد، فرآیندها، دانش و فناوری) در هر زمان، نیاز به جذب و انتشار دانش در سازمان است. برای فرآیندها، می توان با استانداردسازی آنها به این امر دست یافت. برای اطلاعات، این را می توان با گنجاندن دانش در طرح های استاندارد پروژه به دست 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 بهینه سازی منابع، گسترش آگاهی در مورد امنیت

۱. OCTAVE: Operationally Critical Threat, Asset and Vulnerability Evaluation

۲. Joshi & Singh

۳. FAIR: Factor Analysis of Information Risk

۴. NIST RMF: National Institute of Standards and Technology's Risk Management Framework

۵. TARA: Threat Agent Risk Assessment

۶. Dixon

اطلاعات، جایی که می‌توان اطلاعات را جمع‌آوری کرد، جایی که ابزارها را می‌توان یافت و غیره مهم است. برای مثال، با تبدیل امنیت اطلاعات به بخشی از فرهنگ، کارمندان به‌طور خودکار در هنگام شروع یک پروژه جدید، به دنبال دانش امنیت اطلاعات خواهند بود. زیرا بخشی از عملیات عادی آنهاست (لوفن، ۲۰۱۹). به‌طور کلی مدیریت منابع امنیت اطلاعات اصطلاحی است که برای توصیف فرآیندهای برنامه‌ریزی، تخصیص و کنترل منابع امنیت اطلاعات، از جمله افراد، فرآیندها و فناوری‌ها برای بهبود کارایی و اثربخشی راه‌حل‌های کسب و کار استفاده می‌شود. (موسسه حکمرانی فناوری اطلاعات، ۲۰۰۸)

ب-۲-۴ اندازه‌گیری 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 نمی‌کند یا حتی مانع کسب و کار می‌شود، کارمندان راهی برای دور زدن کنترل‌های امنیتی پیدا می‌کنند. این مسیر جایگزین به یک فرآیند سایه تبدیل می‌شود و معمولاً ناامن و مهم‌تر از آن ناشناخته است. بنابراین کنترل‌های امنیتی باید با همکاری تمام لایه‌های سازمان ایجاد شود. عملکرد برنامه امنیتی باید از نظر اثربخشی سنجیده شود. ایجاد یک مورد کسب و کار برای کنترل‌های امنیتی با استفاده از معیارهای سنتی بسیار دشوار است. با این حال، اندازه‌گیری ناملموس نیز مهم است، که برای اندازه‌گیری اثربخشی کامل یک برنامه امنیت اطلاعات لازم است و استفاده از معیارها در امنیت اطلاعات مزایای مختلفی دارد:

- به افزایش مسئولیت‌پذیری کمک می‌کنند، زیرا معیارها به تشخیص اینکه آیا کنترل‌های امنیتی خاص به اشتباه اجرا می‌شوند، اصلاً یا فقط بی‌اثر هستند، کمک می‌کنند. یک معیار خاص می‌تواند پرسنل مسئول معیارهای خاص و ویژگی‌های آن را شناسایی و ردیابی کند.
- کنترل‌های خاص را می‌توان به اهداف و مقاصد استراتژیک سازمان مرتبط کرد و بنابراین برای ارزیابی اثربخشی کل برنامه امنیت اطلاعات مفید است.
- می‌توان از آنها برای نشان دادن انطباق با قوانین، قوانین و مقررات استفاده کرد.
- یک ورودی و بازخورد جدید و قابل‌سنجش برای تخصیص منابع را تشکیل می‌دهند.

(موسسه حکمرانی فناوری اطلاعات، ۲۰۰۸) (لوفن، ۲۰۱۹)

ب-۲-۵ ارائه و ایجاد ارزش

ارائه ارزش جایی است که سرمایه گذاری ها و مدیریت خطر با هم برخورد می کنند. استراتژی ای که یک سازمان برای اجرای مدیریت خطر انتخاب می کند، نقش مهمی در تمام تصمیمات آینده دارد. مقدار مناسبی از سرمایه گذاری های 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، ۲۰۰۸) (ایساکا، ۲۰۱۸). 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 کنترل های امنیت اطلاعات بر سازمان وارد می کنند 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 نظر گرفتن ارزش مالی، اندازه گیری قابلیت جدید خدمات و میزان اعتماد به امنیت اطلاعات (از نظر افراد و فرآیندها) مهم است (لوفن، ۲۰۱۹).

۶. نتیجه گیری و پیشنهاد

سازمان ها باید امنیت اطلاعات را در عملکرد روزمره خود به طور فعال بگنجانند و به طور موثر با تغییرات فناورانه و خطرات فزاینده امنیت سایبری مقابله کنند. وضعیت امنیتی از سازمانی به سازمان دیگر متفاوت است؛ اما به طور کلی برای هر سازمان، صرف نظر از فعالیت کسب و کار آنها، برقراری امنیت اطلاعات یک فعالیت بسیار پیچیده و با ماهیتی پویا است. بنابراین، مستلزم بهبود مستمر، چابکی، پاسخگویی، مسئولیت پذیری و انعطاف پذیری است. لذا توصیه می شود سازمان ها ابتدا اهداف اصلی امنیتی خود را تعیین کنند، سپس روش های مناسب را برای رسمی شدن و اعتبار بخشیدن به مدیریت خود به کار گیرند و در نهایت روش هایی را برای دستیابی

به اهداف خود توسعه دهند.

به طور 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 و مآخذ

الف. منابع فارسی

- آفتابی، نوید (۱۳۹۷). 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 (۱۳۹۲). نقش پیاده سازی 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 استاندارد ایران (۱۳۹۲). استاندارد ایران-ایزو-آی ای سی ۲۷۰۱۴:فناوری اطلاعات - فنون امنیتی -حاکمیت امنیت اطلاعات.
- فقیهی، ابوالحسن و علیزاده، محسن (۱۳۸۴). روایی در تحقیق کیفی. فرهنگ مدیریت ۱۳۸۴ شماره ۹.

ب. منابع انگلیسی

- Al-Ahmad, W., & Mohammad, B. (۲۰۱۲). CAN A SINGLE SECURITY FRAMEWORK ADDRESS INFORMATION SECURITY RISKS ADEQUATELY? *International Journal of Digital Information and Wireless Communications (IJDIWC)* ۲(۳), ۲۲۲-۲۳۰.
- Allen, J. (۲۰۰۵). *Governing for Enterprise Security*, Technical Note. Pittsburgh.
- Awasthi, A. (۲۰۱۹). IT Infrastructure & Enterprise Applications - Organizations Strategy and Planning. *International Journal of Science and Research (IJSR) Volume 9 Issue 4, April 2020*, ۱۵۱۷-۱۵۲۳.
- Bergeron, F., & et al. (۲۰۱۷). A framework for research on information technology governance in SMEs. در *Strategic IT Governance and Alignment in Business Settings*. doi: ۱۰.۴۰۱۸/۹۷۸-۱-۵۲۲۵-۰۸۶۱-۸.ch۰۰۳
- Blakley, B., & et al. (۲۰۰۱). Information security is information risk management. NSPW '۰۱: Proceedings of the ۲۰۰۱ workshop on New security paradigms. doi: ۱۰.۱۱۴۵/۵۰۸۱۷۱,۵۰۸۱۸۷
- CASPUK. (۲۰۲۲). <https://casp-uk.net/casp-tools-checklists/>. Retrieved from www.casp-uk.net.
- Day, G. S., & Schoemaker, P. (۲۰۰۰). Avoiding the Pitfalls of Emerging Technologies. *California Management Review* ۴۲(۲), ۸-۳۳. doi: ۱۰.۲۳۰۷/۴۱۱۶۶۰۳
- de Oliveira Alves, G. d. (۲۰۰۶). *Enterprise Security Governance; A practical guide to implement and control Information Security Governance (ISG)*.
- Dewhurst, M., & Willmott, P. (۲۰۱۴). Manager and machine: the new leadership equation. *McKinsey Quarterly*. Retrieved from <https://www.mckinsey.com/featured-insights/leadership/manager-and-machine>
- Dixon, B. (۲۰۰۹). Understanding the FAIR risk assessment. *Nebraska CERT conference*.
- Dor, D., & Elovici, Y. (۲۰۱۶). A model of the information security investment decision-making process. *Computers & Security* ۶۳, ۱-۱۳.

- Erwin, E. J., & et al. (۲۰۱۱). Understanding Qualitative Metasynthesis: Issues and Opportunities in Early Childhood Intervention Research. *Journal of Early Intervention* ۳۳(۲), ۱۸۶-۲۰۰.
- Gashgari, G., & et al. (۲۰۱۷). A Proposed Best-practice Framework for Information Security. *IoTBDs ۲۰۱۷- ۳rd International Conference on Internet of Things, Big Data and Security* (pp. ۲۹۰-۳۰۱). SCITEPRESS – Science and Technology Publications, Lda.
- George, T. (۲۰۱۳). Risk and Compliance-For Better or Worse? *ISACA Journal - ۲۰۱۳ Volume ۴, ۱۲-۱۵*. Retrieved from <https://www.isaca.org/resources/isaca-journal/past-issues/۲۰۱۳/risk-and-compliance-for-better-or-worse>
- Haes, S., & Grembergen, W. (۲۰۰۸). Analysing the Relationship Between IT Governance and Business/IT Alignment. Proceedings of the ۴th Hawaii International Conference on System Sciences. Waikoloa, HI, USA: IEEE. doi:۱۰.۱۱۰۹/HICSS.۲۰۰۸.۶۶
- Haufe, K., & al, e. (۲۰۱۶). A process framework for information security management. *International Journal of Information Systems and Project Management*, ۲۷-۴۷. doi:۱۰.۱۲۸۲۱/ijispm.۴۰۴۰۲
- ISACA. (۲۰۱۸). COBIT ۲۰۱۹ FRAMEWORK: INTRODUCTION & METHODOLOGY. Retrieved from www.isaca.org/COBITuse
- ITGI. (۲۰۰۶). Information Security Governance: Guidance for Boards of Directors and Executive Management (۲nd ed.). IT Governance Institute
- ITGI. (۲۰۰۷). CobiT ۴.۱. *The IT Governance Institute*. Retrieved from (www.itgi.org)
- ITGI. (۲۰۰۸). *Information Security Governance-Guidance for Information Security Managers*. IT Governance Institute. Retrieved from www.itgi.org
- Joshi, C., & Singh, U. K. (۲۰۱۷). Information security risks management framework – A step towards mitigating security risks in university network. Elsevier; *Journal of Information Security and Applications*, ۱۲۸-۱۳۷. Retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S۲۲۱۴۲۱۲۶۱۶۳۰۱۸۰۶?via=ihDihub>
- Kiesling, E., & et al. (۲۰۱۶). Selecting security control portfolios: a multi-objective simulation-optimization approach. *EURO Journal on Decision Processes* Volume ۴, Issues ۱-۲, ۸۵-۱۱۷.
- Kvale, S. (۱۹۹۶). Interview Views: An Introduction to Qualitative Research Interviewing. Thousand Oaks, CA: Sage Publications.
- Kraus, A. (۲۰۱۸). Developing an Information Security Strategy. The St. Pölten University of Applied Sciences. Retrieved from <http://www.fhstp.ac.at/en>
- Loeffen, F. (۲۰۱۹). 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. (۲۰۱۰). GTAG Information Security Governance. *The Institute of Internal Auditors*, ۱۳۴.
- National Cyber Security Summit Task Force (۲۰۰۴). Information Security Governance : a Call To Action, Corporate Governance Report
- Nazareth, L., & Choi, J. (۲۰۱۵). A system dynamics model for information security management. *Information & Management* Volume ۵۲, Issue ۱, ۱۲۳-۱۳۴.
- Nicho, M. (۲۰۱۸). A Process Model for Implementing Information Systems Security Governance. Information and computer security [online], ۲۶(۱), ۱۰-۲۸. Retrieved from <https://openair.rgu.ac.uk>
- Noblit, G., & Hare, R. (۱۹۸۸). *Meta-ethnography: synthesizing qualitative studies*.
- Nominet. (۲۰۱۹). *LIFE INSIDE THE PERIMETER - Understanding the modern CISO*. NOMINET CYBER SECURITY.
- Ohki, E., & et al. (۲۰۰۷). Information Security Governance Framework. Information Systems

Management ۲۴(۴), ۳۶۱-۳۷۲. doi:۱۰,۱۱۴۵/۱۶۵۵۱۶۸,۱۶۵۵۱۷۰

- Pereira, T., & Santos, H. (۲۰۱۴). Challenges in Information Security Protection. ۱۳th European Conference on Cyber Warfare and Security (ECCWS-۲۰۱۴). The University of Piraeus, Piraeus, Greece.
- Rastogi, R., & von Solms, R. (۲۰۰۶). Information Security Governance-A Re-Definition, Security Management, Integrity, and Internal Control in Information Systems, ۱۹۳, ۲۲۳-۲۳۶.
- Rebollo, O., & et al. (۲۰۱۱). Comparative Analysis of Information Security Governance Frameworks: A Public Sector. 1th European Conference on e-Government (ECEG' 11), Ljubljani, Slovenia, ۱۶- ۱۷, (pp. ۴۸۲ - ۴۹۰).
- Sandelowski, M. (۲۰۰۷). *Handbook for Synthesizing Qualitative Research*. Springer Publishing Company.
- Schinagl, S., & Shahim, A. (۲۰۱۹). What do we know about information security governance? "From the basement to the boardroom": towards digital security governance. *Information & Computer Security*, Vol. ۲۸ No. ۲, ۲۰۲۰, ۲۶۱-۲۹۲. doi:۱۰,۱۱۰۸/ICS-۰۲-۲۰۱۹-۰۰۳۳
- Selig, G. (۲۰۱۶). IT Governance-An Integrated Framework and Roadmap: How to Plan, Deploy and Sustain for Improved Effectiveness. *Journal of International Technology and Information Management Volume ۲۰- Issue ۱*, ۵۵-۷۶.
- Silva, H., & et al. (۲۰۱۹). INFORMATION TECHNOLOGY GOVERNANCE IN SMALL AND MEDIUM. *Journal of Information Systems and Technology Management – Jistem USP- Vol. ۱۷, ۲۰۲۰, e ۲۰۲۰۱۷۰۰۱*. doi:۱۰,۴۳۰۱/S۱۸۰۷-۱۷۷۵۲۰۲۰۱۷۰۰۱
- Simonsson, M., & Johnson, o. (۲۰۰۶). Assessment of IT Governance- A Prioritization of Cobit. *Proceedings of the Conference on Systems Engineering Research*.
- Usman, S. (۲۰۱۹). MIT Governance Implementation in Enterprise: A Review. *IJRECE (INTERNATIONAL JOURNAL OF RESEARCH IN ELECTRONICS AND COMPUTER ENGINEERING) VOL. ۷ ISSUE ۲ Apr-June ۲۰۱۹*, ۳۱۲۹-۳۱۳۴.
- Whitman, M. E., & Mattord, H. J. (۲۰۱۲). Information Security Governance for the Non-Security Business Executive. *Journal of Executive Education*, ۱۱(۱) (۲۰۱۲), ۹۷-۱۱۱.
- Williams, P. (۲۰۰۱). Information Security Governance. Information Security Technical Report ۶(۳), ۶۰-۷۰. doi:۱۰,۱۰۱۶/S۱۳۶۳۴۱۲۷(۰۱)۰۰۳۰۹۰
- Williams, S., & et al. (۲۰۱۳). Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. *Electron Markets* (۲۰۱۳) ۲۲, ۳۴۱-۳۵۴. doi:۱۰,۱۰۰۷/s۱۲۵۲۵-۰۱۳-۰۱۳۷-۲
- Zimmer, L. (۲۰۰۶). Qualitative meta-synthesis: a question of dialoguing with texts. *Journal of Advanced Nursing* ۵۲(۲), ۳۱۱-۳۱۸. doi:۱۰,۱۱۱۱/j.۱۳۶۵-۲۶۴۸,۲۰۰۶,۰۳۷۲۱.x

