عوامل کلیدی ارتقای توانمندی فناورانه امنیت سایبری در زیرساخت‌های حیاتی

مریم بهی‌فر

دانشجوی دکتری مدیریت تکنولوژی، گروه مدیریت تکنولوژی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران.

محمدرضا رضوی*[1]

استادیار، گروه مدیریت تکنولوژی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران.

پریوش جعفری

دانشیار، گروه مدیریت آموزشی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران

مدیریت اطلاعات

دوره ۱۱، شماره ۱

بهار و تابستان ۱۴۰۴

چکیده: پیشرفت سریع فناوری اطلاعات و ارتباطات، سبب شده تا شرکت‌های خدمات‌دهنده بعنوان یک زیرساخت حیاتی با شیوع، شدت و پیچیدگی فزاینده‌ای از حملات سایبری روبرو گردند که به تمرکز بیشتری بر امنیت سایبری نیاز دارد. از اینرو، پژوهش حاضر با استفاده از رویکرد کیفی چند روشی (تحلیل مضمون و دلفی فازی) مضامین کلیدی برای ارتقای توانمندی فناورانه امنیت سایبری استخراج و دسته‌بندی و تفسیر نموده است. براین اساس، نخست با مطالعه و تحلیل ادبیات توانمندی فناوری اطلاعات و مصاحبه‌های تخصصی نیمه‌ساختاریافته با ۱۰ نفر از مدیران و متخصصان صنعتی و دانشگاهی و استفاده از رویکرد تحلیل مضمون، توانمندی‌های فناورانه در حوزه امنیت سایبری را در ۵ مضمون سازمان‌دهنده و ۳۶ مضمون پایه شناسایی و دسته‌بندی نموده است. سپس، پرسشنامه دلفی فازی در بین ۲۵ نفر از خبرگان توزیع و اهمیت هر یک از معیارها تعیین گردید. به دلیل تکراری بودن یا ادغام با سایر عامل‌ها، ۹ عامل از مجموعه عامل‌های کلیدی توانمندی فناورانه امنیت سایبری غربال گردیدند و درنهایت، ۲۷ مضمون پایه یا عامل کلیدی تایید شدند. نتایج نشان دادند که توانمندی فناورانه امنیت سایبری از ۵ مضمون سازمان‌دهنده شامل توانمندی منابع‌انسانی با ۴ مضمون پایه، توانمندی فرایندهای سازمانی با ۳ مضمون پایه، توانمندی فنی و زیرساختی امنیتی با ۹ مضمون پایه، توانمندی راهبردی و مدیریتی با ۶ مضمون پایه، توانمندی امنیت ذی‌نفعان کلیدی با ۵ مضمون پایه تشکیل شده است.

کلیدواژه‌ها: فناوری اطلاعات، امنیت سایبری، توانمندی فناورانه، نفت و گاز.

---

[1] نویسندهٔ مسئول: mrazzavi@yahoo.com

مقدمه

توسعه و گسترش سریع فناوری اطلاعات و ارتباطات، شرکت‌ها را با خطرات امنیتی بسیاری مواجه کرده است. آسیب‌پذیری‌های سایبری به تهدیدی جدی برای سازمان‌های دولتی و شرکت‌های خصوصی تبدیل شده‌اند که موجب سرمایه‌گذاری‌های چند میلیارد دلاری در سیستم‌ها و نرم‌افزارها برای شناسایی این تهدیدها شده است (آکسوی[۱]، ۲۰۲۳؛ ۲۰۲۴).

صنعت نفت و گاز زیرساختی حیاتی برای کشور ایران محسوب می‌شود که اختلال یا آسیب به آن می‌تواند تأثیرات مضر قابل‌توجه‌ای بر اقتصاد، نظم اجتماعی و امنیت ملّی کشور داشته باشد (بهی‌فر و همکاران، ۱۴۰۲؛ قره‌باجاک[۲] و همکاران، ۲۰۱۶). شواهد تاریخی از حملات مخرب عمدی (حملات امنیتی) که تأسیسات نفت و گاز بخصوص فراساحل (ایانی[۳] و همکاران، ۲۰۲۱آ؛ کورنر[۴]، ۲۰۱۱؛ هارل[۵]، ۲۰۱۲) و فعالیت‌های مرتبط (ژو[۶] و همکاران، ۲۰۲۱؛ منگ[۷] و همکاران، ۲۰۲۱؛ جان[۸] و همکاران، ۲۰۱۶؛ ژو، ۲۰۲۲) را هدف قرار می‌دهند، وجود دارد. این حملات توسط طیف وسیعی از گروه‌ها، از معترضان زیست‌محیطی گرفته تا ارتش کشورهای متخاصم و سازمان‌های تروریستی انجام می‌شود. انگیزه‌های دشمنان ممکن است سود مالی، برهم‌زدن تعادل اقتصادی و سیاسی، انتقام، چالش یا نگرانی‌های زیست‌محیطی باشد (کاشوبسکی[۹]، ۲۰۱۱؛ باجپای و گوپتا[۱۰]، ۲۰۰۷) وجود مقادیر زیادی از مواد خطرناک (نفت خام و گاز طبیعی فرآوری‌شده)؛ اثرات این حملات امنیتی را تشدید می‌نماید زیرا می‌توانند زیان‌های قابل‌ملاحظه‌ای بر انسان، محیط‌زیست و دارایی‌ها داشته باشند که با حوادث ناشی از سلامت، ایمنی و بهداشت قابل مقایسه است (ایانی و همکاران، ۲۰۲۱ب؛ واسیلوف[۱۱]، ۲۰۱۶؛ استاین اوسلر[۱۲] و همکاران، ۲۰۰۸). می‌توان به حوادث شناخته‌شده‌ای اشاره نمود: حمله سایبری به وزارت نفت و تعدادی از شرکت‌های تابعه کشور در سال ۱۳۹۱ هجری شمسی معادل با سال ۲۰۱۲ میلادی با بدافزار فیلم که نه‌تنها سبب قطع دسترسی چند روزه اینترنت برای کارمندان وزاتخانه نفت و کارکنان شرکت ملّی نفت ایران، شرکت‌های پتروشیمی، پایایشگاه و توزیع شد، بلکه، اینترنت در خارگ، بهرگان، سیری، لاوان، قشم و کیش مسدود گردید (واعظی‌نژاد و مقدس، ۱۳۹۴). همچنین، در سال ۱۳۸۹ هجری شمسی معادل با سال ۲۰۱۰ میلادی واردکردن بدافزار استاکس‌نت[۱۳] در نیروگاه اتمی نطنز ایران که محدود به این نیروگاه باقی نمانده و در سراسر جهان پخش

---

[1] Aksoy
[2] Karabacak
[3] Iaiani
[4] Cordner
[5] Harel
[6] Zhou
[7] Meng
[8] John
[9] Kashubsky
[10] Bajpai & Gupta
[11] Vasilev
[12] Steinhäusler
[13] Stuxnet

شد. این بدافزار نخستین بدافزار در رده نظامی بود که بصورت فیزیکی منجر به خرابی و از کارافتادگی «سانتریفیوژها» شد. (کافی، ۱۳۹۹؛ بیگزاده، ۱۴۰۴). حمله با استفاده از بدافزار دوکو در سال ۱۳۹۰ هجری شمسی معادل با سال ۲۰۱۱ میلادی در سطح غرب آسیا و ایران گسترش یافت. این بدافزار برای سرقت اطلاعات استفاده شد (کافی، ۱۳۹۹). وقایع فوق تأیید می‌کنند که امنیت زیرساخت‌های حیاتی از جمله تأسیسات نفت و گاز باید یک نگرانی بزرگ در نظر گرفته شوند. به گفته پروگولاکیس و نیکیتاکوس[1] (۲۰۱۹)، امنیت تأسیسات نفت و گاز به‌این‌صورت تعریف می‌شود «فرآیندی که در آن دارایی‌های عملیاتی (اکتشاف و تولید) و مهندسی بطور فعال و غیرفعال توسط اقدامات و قوانین سختگیرانه فیزیکی و عملیاتی برای حصول اطمینان از انعطاف‌پذیری و کاهش تخریب مرتبط با نقض امنیت محافظت می‌شوند.»

از اوایل دهه ۱۹۸۰ شرکت‌های نفت و گاز شروع به استفاده از فناوری‌های دیجیتالی، با تمرکز بر درک بهتر از منابع، بهبود پتانسیل تولید مخزن، ارتقای سلامت، ایمنی و بهداشت و افزایش بهره‌وری عملیاتی نمودند. در ادامه این روند، از دهه ۱۹۹۰ و اوایل قرن حاضر نیز در سراسر جهان موجی از طرح‌های نفتی دیجیتال بوجود آمده است (مزاروش[2]، ۲۰۱۷). اگرچه این زیرساخت‌های زیربنایی مدت‌ها پیش از گسترش استفاده از اینترنت و فناوری‌های سایبری وجود داشته‌اند، اما سیستم‌های سایبری آنها را در معرض تهدیدهای سایبری قرار داده‌اند (آکسوی، ۲۰۲۳). همگرایی بین سیستم‌های فناوری‌های عملیاتی (OT) صنعتی و فناوری‌ها و شبکه‌های مبتنی بر فناوری اطلاعات (IT)، مزایای تجاری بالقوه بسیاری را در صنعت نفت و گاز به دنبال داشته است. همگرایی شبکه IT/OT می‌تواند به کاهش فضای مورد نیاز، حذف سخت‌افزار فیزیکی، کوتاه کردن زمان استقرار، صرفه‌جویی در هزینه، افزایش عملکرد و کاهش بخش فناوری‌های عملیاتی و اطلاعاتی کمک کند (فورتی‌نت[3]، می ۲۰۲۳). با این‌حال، همگرایی مورد بحث (ترکیب سیستم‌های فناوری‌های عملیاتی صنعتی و فناوری‌ها و شبکه‌های مبتنی‌بر فناوری اطلاعات)، در زیرساخت‌های حیاتی فناوری‌های عملیاتی سنتی که از انواع حملات سایبری رایج ایمن نگه داشته می‌شدند، شکاف ایجاد می‌کند. در نتیجه اتصالات اخیر، سه چهارم سازمان‌های مبتنی‌بر فناوری‌های عملیاتی دست‌کم یک مورد نفوذ را در سال ۲۰۲۲ گزارش کردند. بدافزار (۵۶ درصد) و فیشینگ (۴۹ درصد) از شایع‌ترین حملات بودند و تقریباً یک‌سوم شرکت‌ها گزارش دادند که قربانی باج افزار هستند (فورتی‌نت، اکتبر ۲۰۲۳).

یک حمله سایبری در مقایسه با حملات معمولی مزایای آشکاری همانند ناشناس بودن، قابل انکار بودن، مقرون‌به‌صرفه بودن و سهولت استفاده دارد. درواقع، تهدیدات سایبری براحتی و بدون زحمت، راه را برای حملات مضر علیه دارایی‌های زیرساختی حیاتی هموار می‌کنند (قره‌باجاک و همکاران، ۲۰۱۶). صنعت نفت و گاز، بطور ویژه یک هدف جذاب برای حملات سایبری در سراسر جهان است. حمله سایبری به زیرساخت‌های خشکی و فراساحلی نفت و گاز می‌تواند آسیب فیزیکی، زیست‌محیطی، اقتصادی و اختلال‌های گسترده‌ای در عرضه و بازارهای نفت و گاز ایجاد کند (فورتی‌نت، اکتبر ۲۰۲۴). در ایران نیز،

[1] Progoulakis & Nikitakos
[2] Meszaros
[3] Fortinet

صنعت نفت و گاز از بخش‌های اصلی اقتصاد کشور بوده و بخش قابل‌توجه‌ای از تولید ناخالص داخلی را تولیدات بالادست نفت و گاز تشکیل می‌دهند. با توجه به شرایط اقتصادی، سیاسی و ژئوپلیتیکی ایران و اهمیت صنعت نفت و گاز در کشور امکان حمله دشمنان با هدف آسیب به این صنعت همواره وجود دارد. از اینرو، صنعت مذکور همواره در معرض انواع تهدیدهای سایبری، خرابکاری، جاسوسی و انفجار قرار دارد. بعلاوه، مطابق با الزام‌های ابلاغی پدافند غیرعامل کشور (صولت رفیعی و همکاران، ۱۴۰۳) و اجرای آن، می‌توان گفت که ارتقای توانمندی فناورانه امنیت سایبری در بالادست صنعت نفت و گاز از اهمیت ویژه‌ای برخوردار است. بنابراین، مقاله حاضر به شناسایی عوامل کلیدی ارتقای توانمندی فناورانه امنیت سایبری در بالادست صنعت نفت و گاز ایران پرداخته است. از این‌جهت، در بخش دوم (مبانی نظری) به تشریح توانمندی فناورانه شرکت‌ها بر مبنای دیدگاه منبع‌محور و گسترش آن به مباحث فناوری اطلاعات و امنیت سایبری در بالادست صنعت نفت و گاز پرداخته می‌شود. بخش سوم، به مبانی فلسفی پژوهش با رویکرد کیفی، مشارکت‌کنندگان، نمونه و نحوه گردآوری داده‌ها و ابزار پژوهش و نحوه تجزیه و تحلیل داده‌ها (تحلیل مضمون و دلفی فازی) می‌پردازد. بخش چهارم، با استفاده از تشریح و استفاده از روش تحلیل مضمون ابعاد و مولفه‌های متغیرهای مدل تعیین و با بکارگیری دلفی فازی غربالگری و نهایی می‌گردند. بخش پنجم، به بحث و نتیجه‌گیری می‌پردازد.

مبانی نظری

حملات سایبری در سراسر جهان بطور گسترده‌ای درحال افزایش بوده و چالش‌های مهمی را برای شرکت‌ها بوجود آورده است. بنابراین، شرکت‌ها برای دفاع از محیط‌های اطلاعاتی خود در برابر این عامل تهدید مداوم و قدرتمند، همواره در تلاش هستند (جانسون[1] و همکاران، ۲۰۱۷). اکنون امنیت سایبری دیگر یک مشکل صرفا فنی نبوده، بلکه یک چالش راهبردی در سطح سازمان محسوب می‌شود. نظرسنجی پی‌دبلیوسی[2] در سال ۲۰۲۱ نشان داد که ۹۵ درصد از مدیران عامل بیان کردند که امنیت سایبری یک تهدید بزرگ برای رشد است، که نسبت به سال قبل ۶۱ درصد افزایش یافته است (پی.دبلیو.سی.، ۲۰۲۱). امنیت سایبری «شامل تصمیم‌های استراتژیک درباره مبادلات ضروری است» زیرا مشکل باید در کل یک سازمان که نیاز به تایید و پشتیبانی اجرایی دارد به اشتراک گذاشته شود (سی.اس.آ.[3]، ۲۰۲۱). علاوه‌براین، با توجه به ظهور عوامل‌تهدید سایبری سازمان‌یافته و پیچیده، نقش حیاتی «هوشمندی تهدیدات سایبری (CTI)» به رسمیت شناخته شده است (برندت و اوفوف[4]، ۲۰۲۰).

[1] Johnson
[2] PwC
[3] CSA
[4] Berndt & Ophoff

زیرساخت‌های حیاتی

زیرساخت‌های حیاتی یکی از مفاهیم اساسی در حوزه حکمرانی خوب[1] است که در میان دارایی‌ها و فرآیندهای گسترده حفاظت از منابع کمیاب را در اولویت قرار می‌دهد. زیرساخت‌های حیاتی و چگونگی وابستگی آنها به یکدیگر مطابق با سیاست‌های کلان و شرایط هر کشور متفاوت می‌باشد. همانطور که در قطعنامه ۲۳۴۱ (۲۰۱۷)، تأکید شده است «هر کشور مشخص می‌کند که چه چیزی زیرساخت‌های حیاتی آن را تشکیل می‌دهد.» (نعمت‌پور و همکاران، ۱۴۰۰؛ اختری و همکاران، ۱۴۰۲ الف و ب؛ صولت رفیعی و همکاران، ۱۴۰۳).

بر اساس طرح راهبردی حفاظت از زیرساخت‌های کشور ایران مصوب شصت و ششمین جلسه کمیته دائمی (شورای عالی) پدافند غیرعامل در تاریخ ۱۴۰۱/۰۶/۲۹؛ مطابق با ماده ۱، بند ۴ آن، حوزه‌های با اهمیت بالا به هر یک از حوزه‌های ۱-انرژی، ۲-آب، ۳-غذا و کشاورزی، ۴-حمل و نقل، ۵-بهداشت و سلامت، ۶-دفاعی و امنیتی، ۷-صنعت، ۸-رسانه، ۹-هسته‌ای، ۱۰-فضا، ۱۱جمعیت، ۱۲-حاکمیتی، ۱۳-خدمات ضروری و فوریتی، ۱۴-پولی و مالی، ۱۵-ارتباطات و فناوری اطلاعات، حوزه‌های با اهمیت بالا گفته می‌شود که ۸ حوزه ۱-انرژی، ۲-آب، ۳- ارتباطات و فناوری اطلاعات، ۴-حمل و نقل، ۵-بهداشت و سلامت، ۶- غذا و کشاورزی، ۷- دفاعی و امنیتی، و ۸-حاکمیتی به‌عنوان حوزه‌های کلیدی از منظر پدافند غیرعامل دسته‌بندی می‌شوند. همچنین، زیرساخت‌های حیاتی کشور را از منظر سایبری می‌توان به پنج زیر بخش انرژی، حمل و نقل، ارتباطات و فناوری اطلاعات، مالی و سلامت تقسیم نمود. زیر ساخت انرژی خود به ۷ بخش نفت، گاز، پتروشیمی برق، آب، کنترل صنعتی و انرژی اتمی تقسیم می‌شود (صولت رفیعی و همکاران، ۱۴۰۳).

امنیت سایبری

امنیت سایبری درحال‌ظهور از امنیت اطلاعات سنتی است. زیرا سیستم‌ها و دستگاه‌های اطلاعاتی بطور فزاینده‌ای به اینترنت متصل می‌شوند و اغلب در فضای ابری کار می‌کنند، که آسیب‌پذیری‌های بیشتر و تقاضای بالایی برای امنیت ایجاد می‌کند (بایکلوی[2] و همکاران، ۲۰۲۰). با توجه به ماهیت درحال تحول آن، هیچ تعریف واحدی از امنیت سایبری وجود ندارد. شاتز[3] و همکاران (۲۰۱۷) با استفاده از تحلیل معنایی ۲۸ تعریف از امنیت سایبری، امنیت سایبری را «رویکرد و اقدامات مرتبط با فرآیندهای مدیریت ریسک امنیتی که توسط سازمان‌ها و دولت‌ها برای محافظت از محرمانه بودن، یکپارچگی و در دسترس‌بودن داده‌ها و دارایی‌های مورد استفاده در فضای سایبری دنبال می‌شود» تعریف کرده‌اند. مفهوم‌سازی جامع آنها از امنیت سایبری، مصنوعات سازمانی از دستورالعمل‌ها، خط‌مشی‌ها و زیرساخت‌های فناورانه امنیت سایبری تا فرآیندها، اقدامات و آموزش را پوشش می‌دهد (یئو[4] و همکاران، ۲۰۲۲).

---

[1] Good Government
[2] Baikloy
[3] Schatz
[4] Yeoh

بطور معمول، امنیت سایبری «اقداماتی است که برای محافظت از رایانه یا سیستم شبکه (مانند اینترنت) در برابر دسترسی یا حمله غیرمجاز انجام می‌شود» (مریام-وبستر[1]، ۲۰۲۳). اولین مطالعه جامع منتشر شده که زمینه را برای حوزه امنیت سایبری فراهم کرد، یک گزارش فنی در سال ۱۹۷۰ به نام «کنترل امنیتی برای سیستم‌های کامپیوتری» بود (وار[2]، ۱۹۷۰). بااین‌حال، امنیت سایبری در سال‌های اخیر با افزایش حملات سایبری توجه بیشتری را به خود جلب کرده است.

از نظر فنی، بسیاری از انواع حملات سایبری از آسیب‌پذیری‌ها، ضعف‌ها و فرصت‌های مختلف ناشی می‌شوند. اساساً، اولین راه برای طبقه‌بندی حملات، تفکیک آنها به دو ویژگی متمایز، «تهدیدهای مخرب» و «تهدیدهای غیرعمدی» است. تهدیدات مخرب می‌تواند توسط مهاجمان خارجی، کارمندان مخرب یا کارمندان حریص که به دنبال فروش داده‌های شرکت برای کسب درآمد سریع هستند، ایجاد شود. تهدیدهای غیرعمدی یا ناخواسته توسط کارکنان بی‌دقتی ایجاد می‌شود که بدون درنظرگرفتن عواقب اقدامات خود عمل می‌کنند. کلیک کردن بر روی ایمیل‌های منابع ناشناس، باز کردن وب‌سایت‌هایی که محصولات جذاب را نشان می‌دهند، یا باز کردن ایمیل‌هایی خارج از شبکه اداری نمونه‌های بارز چنین حملاتی هستند (ساندو[3]، ۲۰۲۱).

توانمندی فناوری اطلاعات

دیدگاه منبع‌محور (RBV) در بسیاری از مطالعه‌ها برای بررسی تأثیر سرمایه‌گذاری در فناوری اطلاعات بر عملکرد شرکت استفاده شده است. پژوهشگران نشان داده‌اند که توانایی یک شرکت برای استفاده مؤثر از سرمایه‌گذاری در فناوری اطلاعات همراه با توسعه توانمندی مربوطه، می‌تواند عملکرد شرکت را بهبود بخشد (سانتانام و هارتونو[4]، ۲۰۰۳). توانمندی فناوری اطلاعات به توانایی سازمان برای شناسایی، بسیج و استقرار دارایی‌ها و منابع فناوری اطلاعات که نیازهای کسب و کار را برآورده می‌سازد و بهبود فرآیندهای کسب و کار با بکارگیری فناوری اطلاعات و ارائه پشتیبانی طولانی مدت برای سیستم‌های مبتنی بر فناوری اطلاعات را به دنبال دارد، اشاره دارد (کریمی[5] و همکاران، ۲۰۰۷). یک سازمان با توانمندی فناوری اطلاعات قوی می‌تواند دارایی‌ها و منابع فناوری اطلاعات مختلف را برای منافع سازمانی و ارزش‌های تجاری مختلف یکپارچه و هماهنگ کند (وید و هالند[6]، ۲۰۰۴؛ یئو و همکاران، ۲۰۲۲).

پژوهشگران نشان داده‌اند که توانمندی فناوری اطلاعات یک توانمندی سازمانی ضروری است (وید و هالند، ۲۰۰۴). بر اساس دیدگاه منبع‌محور (بارنی[7]، ۱۹۹۱؛ ۲۰۰۱)، توانمندی‌های سازمانی منابع شرکت‌ها هستند که می‌توانند بر مزیت رقابتی آنها تأثیر بگذارند. توانمندی‌های سازمانی توانایی یک شرکت برای

[1] Merriam-Webster
[2] Ware
[3] Sandhu
[4] Santhanam & Hartono
[5] Karimi
[6] Wade & Hulland
[7] Barney

یکپارچه‌سازی دارایی‌ها و منابع سازمانی و انجام وظایف بطور قابل اعتماد است (گرانت و ورونا[1]، ۲۰۱۵) توانمندی‌های سازمانی می‌تواند عملکردی یا پویا باشد. نمونه‌هایی از توانمندی‌های عملکردی شامل توانمندی عملیاتی، توانمندی بازاریابی و فروش و توانمندی منابع انسانی است (گرانت[2]، ۱۹۹۶). توانمندی‌های پویا، توانمندی‌های درجه بالاتری هستند که توانمندی‌های عملکردی مرتبه پایین‌تر را مجدداً پیکربندی و تجدید می‌کنند. مانند توانمندی یادگیری و توانمندی توسعه موثر محصول (ایزنهارت و مارتین[3]، ۲۰۰۰؛ تیس[4] و همکاران، ۱۹۹۷). توانمندی‌های سازمانی شامل روال‌ها و فرآیندهایی است که دارای الگوهای تکرارپذیری از فعالیت‌ها هستند و بطور معمول، بازیگران و دارایی‌های متعددی را در شرکت درگیر و ادغام می‌کنند (بکر[5]، ۲۰۰۴؛ فلین و فاس[6]، ۲۰۰۹).

از آنجایی که روال‌ها و فرآیندها، پدیده‌هایی پیچیده و چندعاملی هستند، توانمندی‌هایی که ایجاد می‌کنند می‌توانند وابسته به مسیر، مبهم یا از نظر اجتماعی پیچیده باشند، بنابراین تقلید برای رقبا دشوار می‌شود. باتوجه‌به دیدگاه منبع‌محور، به‌دلیل تقلیدناپذیری و غیرقابل‌جایگزینی توانمندی‌های سازمانی، منابع ارزشمندی هستند که به سازمان‌ها کمک می‌کنند مزیت رقابتی را حفظ کنند (پترافت[7]، ۱۹۹۳). توانمندی فناوری اطلاعات از دیدگاه منبع‌محور و توانایی سازمانی (بارنی، ۱۹۹۱؛ ۲۰۰۱) برای توضیح ارزش دارایی‌های فناوری اطلاعات استفاده می‌کند. پیکربندی مناسب دارایی‌های فناوری اطلاعات در ترکیب با سایر دارایی‌های سازمانی مکمل (وید و هالند، ۲۰۰۴؛ بهارادواج[8]، ۲۰۰۰) توانمندی فناوری اطلاعات را تشکیل می‌دهد که ارزشمند، نادر (کمیاب)، غیرقابل‌جایگزینی و غیرقابل‌تقلید هستند، بنابراین مزیت رقابتی پایداری را برای شرکت‌ها فراهم می‌کنند. مفهوم‌سازی‌های مختلفی از توانمندی‌های فناوری اطلاعات وجود دارد. ماتا[9] و همکاران (۱۹۹۵) سه بعد از توانمندی فناوری اطلاعات را مفهوم‌سازی کردند: فناوری اختصاصی، مهارت‌های فنی فناوری اطلاعات و مهارت‌های مدیریت فناوری اطلاعات. بات و گروور[10] (۲۰۰۵) سه بعد توانمندی فناوری اطلاعات را پیشنهاد کردند: زیرساخت فناوری اطلاعات، توانمندی‌های مدیریت فناوری اطلاعات (یعنی تجربه تجاری فناوری اطلاعات و روابط تجاری) و توانمندی‌های پویا. ملویل[11] و همکاران با بررسی کامل ادبیات پیشنهاد می‌کنند که توانمندی فناوری اطلاعات شامل منابع فنی فناوری اطلاعات، منابع انسانی فناوری اطلاعات و منابع سازمانی مکمل است. شرکت‌ها می‌توانند با بهره‌گیری کامل از توانمندی‌های فناوری اطلاعات موجود خود، مزیت و عملکرد رقابتی خود مانند عملکرد

---

[1] Grant & Verona
[2] Grant
[3] Eisenhardt & Martin
[4] Teece
[5] Becker
[6] Felin & Foss
[7] Peteraf
[8] Bharadwaj
[9] Mata
[10] Bhatt & Grover
[11] Melville

مالی و عملکرد عملیاتی را بهبود بخشند (بات و گروور، ۲۰۰۵؛ سانتانام و هارتونو، ۲۰۰۳). این اثر توانمندساز می‌تواند مستقیم یا غیرمستقیم از طریق بهبود توانمندی‌های سازمانی، مانند چابکی سازمانی و یادگیری سازمانی باشد (چن[۱] و همکاران، ۲۰۱۴؛ لو و رامامورتی[۲]، ۲۰۱۱.چاکراوارتی[۳] و همکاران، ۲۰۱۳). توانمندی فناوری اطلاعات برای مطالعه مصنوعات مختلف فناوری اطلاعات مانند توانمندی تجارت الکترونیکی الکترونیکی (ژوانگ و لدرر[۴]، ۲۰۰۶)، توانمندی رسانه‌های اجتماعی (وانگ و کیم[۵]، ۲۰۱۷)، توانمندی تجزیه‌وتحلیل داده‌های کلان (گوپتا و جورج[۶]، ۲۰۱۶)، توانمندی هوش مصنوعی (میکالف و گوپتا[۷]، ۲۰۲۱)، و توانمندی عمومی فناوری اطلاعات (یون[۸]، ۲۰۱۱)، استفاده شده است. بااین‌حال، هنوز مفهومی از توانمندی امنیت سایبری وجود ندارد. چند مطالعه توانمندی امنیتی را بررسی کرده‌اند (لی و هوانگ[۹]، ۲۰۱۷؛ محمد و بده[۱۰]، ۲۰۱۹)، اما، مبنای نظری این مطالعات مدل بلوغ توانمندی (پاولک[۱۱]، ۲۰۰۹) است که بطور عمده یک مدل در سطح فرآیند بوده که تمام جنبه‌های مدیریت امنیت سایبری را پوشش نمی‌دهد.

روش پژوهش

برای دستیابی به هدف پژوهش از رویکرد کیفی چند روشی مطابق کراسول[۱۲] (۲۰۱۴) و سیلورمن[۱۳] (۲۰۲۰)، استفاده شد. همانطور که مایک-مایر[۱۴] (۲۰۲۰)، استدلال می‌کند، استفاده از رویکردهای روش‌شناختی کیفی مختلف، دانشی را فراهم می‌آورد که در غیراین‌صورت رسیدن به آن برای پژوهشگر قابل دسترس نبود. به‌همین‌دلیل، استربرگ[۱۵] (۲۰۰۲)، «طرح‌های پژوهشی که شامل راهبردهای پژوهشی متعددی باشند را قوی‌ترین آنها می‌داند». بنابراین، با توجه به جنبه اکتشافی پژوهش حاضر، تجزیه‌وتحلیل اسناد با مصاحبه‌های نیمه‌ساختاریافته با استفاده از روش تحلیل مضمون همراه شد، تا همانطور که ساد-بک[۱۶] (۲۰۰۴)، گفته است از ارائه «تنها یک تصویر جزئی و محدود، بدون پیوند به دنیای واقعی» خودداری گردد. براساس، هستی‌شناسی واقع‌گرا، با استفاده از روش تحلیل مضمون مبتنی‌بر راهبرد استقرای تحلیلی، به شناسایی، تحلیل و تبیین الگوهای موجود در داده‌های کیفی بدست آمده از بررسی ادبیات و مصاحبه‌های نیمه‌ساختاریافته با خبرگان پرداخته شد. سپس، با استفاده از دلفی فازی غربال گردید

---

[1] Chen
[2] Lu & Ramamurthy
[3] Chakravarty
[4] Zhuang & Lederer
[5] Wang & Kim
[6] Gupta & George
[7] Mikalef & Gupta
[8] Yoon
[9] Le & Hoang
[10] Mohammed & Bade
[11] Paulk
[12] Creswell
[13] Silverman
[14] Mik-Meyer
[15] Esterberg
[16] Sade-Beck

گراف ۱: مراحل و گام‌های پژوهش

تحلیل مضمون

برای شناخت عوامل کلیدی ارتقای توانمندی فناورانه امنیت سایبری در بالادست صنعت نفت و گاز، همراه با مرور منابع کتابخانه‌ای برای بررسی ادبیات و پیشینه پژوهش، مصاحبه‌های تخصصی نیمه‌ساختاریافته‌ای نیز در پاییز سال ۱۴۰۳ انجام شد. که از میان مدیران و متخصصان صنعتی و دانشگاهی انتخاب شدند. نمونه‌گیری از میان افراد جامعه که شامل خبرگان و آگاهان کلیدی که از باسابقه‌ترین و آگاه‌ترین افراد در حوزه فناوری اطلاعات و ارتباطات و امنیت شبکه (دارای سابقه آموزشی-پژوهشی، مدرک کارشناسی ارشد یا دکتری با تحصیلات دانشگاهی مرتبط، سابقه مدیریتی حداقل سه سال در شرکت‌های حوزه نفت و گاز) به صورت غیراحتمالی[1] و هدفمند[2] با استراتژی نمونه‌گیری متوالی[3] از نوع گلوله برفی[4]

[1] Non-probability Sampling
[2] Purposive Sampling
[3] Sequential Sampling
[4] Snow Ball

که در جهت بیشینه‌سازی تفاوت برای مفاهیم ایجاد شده حرکت کرد و تا اشباع نظری[1] ادامه یافت که در نهایت، ۱۰ مصاحبه انجام شد. در این مرحله پیش از شروع مصاحبه ۴ پرسش باز در زمینه چالش‌ها و پیچیدگی‌های امنیت و تهدید سایبری در بالادست صنعت نفت و گاز، توانمندی‌های مورد نیاز و راهبردهای مقابله و پیشگیری تهدیدها و حملات سایبری در نظر گرفته و در طول فرآیند مصاحبه با توجه به نظرات خبرگان و تحلیل‌ها سوال‌های جدیدی نیز مطرح شد. تمرکز مصاحبه‌ها بر شناسایی توانمندی‌های فناورانه امنیت سایبری در برابر حملات و تهدیدهای بالادست صنعت نفت و گاز قرار داشت. برای تجزیه و تحلیل اسناد و مصاحبه‌ها، عناوین آشکار و پنهان جستجو، سپس تفسیر و برمبنای هدف در دسته‌های معنادار طبقه‌بندی شده و براساس دیدگاه آترایدِ-استیرلینگ[2] (۲۰۰۱)، مضامین پایه (کدها و نکات کلیدی متن)، سازمان‌دهنده (مضامین بدست آمده از ترکیب و تلخیص مضامین پایه) و فراگیر (مضامین عالی دربرگیرنده اصول حاکم بر متن به‌مثابه کل) شکل گرفتند. طبق دیدگاه بروکس[3] و همکاران (۲۰۱۸)، برای تعیین روایی و پایایی علاوه‌براین‌که مضامین فراگیر، سازمان‌دهنده و پایه با مطالعه مبانی نظری، پیشینه و اهداف پژوهش انتخاب و تایید شدند، نظرات و رهنمودهای گروهی از خبرگان نیز لحاظ و جرح و تعدیل نهایی بعمل آمد. همچنین از «بازخورد مشارکت‌کنندگان» و «تطابق همگونی» استفاده شد (بهی‌فر و همکاران، ۱۴۰۲) برای تجزیه‌وتحلیل مصاحبه‌ها از نرم‌افزار MAXQDA2024 بهره گرفته شد.

در ادامه، و پس از شناسایی عوامل کلیدی توانمندی فناورانه امنیت سایبری، بمنظور تعیین اهمیت و اعتبارسنجی معیارهای تصمیم‌گیری، از اجماع دیدگاه و دانش تخصصی خبرگان استفاده و روش دلفی فازی و نرم‌افزارهای Excel 2023 و Matlab 2024 بکار برده شده است.

روش دلفی فازی (FDM)

هدف از بکارگیری روش دلفی، غربالگری و تعیین اهمیت هر از عوامل کلیدی ارتقای توانمندی امنیت سایبری برای بدست آوردن مهمترین آنها با استفاده از نظر خبرگان در دورهای متوالی است (آریا[4] و همکاران، ۲۰۲۰). مراحل زیر برای انجام روش دلفی فازی طی شده است:

پرسشنامه‌ای با ۳۶ سوال (هر عامل بعنوان یک سوال) بصورت طیف لیکرت ۹ گزینه‌ای در بین خبرگان توزیع گردید. پس از توزیع و گردآوری پرسشنامه‌ها، جهت تعیین مهم‌ترین عامل‌ها و مشخص نمودن اهمیت آنها از روش دلفی فازی استفاده شد، در این مرحله پاسخ هر یک از مشارکت‌کنندگان با استفاده از روش دلفی فازی تجزیه‌وتحلیل شد و درنهایت، میانگین قطعی بدست آمده نشان‌دهنده شدت موافقت خبرگان با هرکدام از عوامل پژوهش می‌باشد.

گام ۱: پرسشنامه دلفی در زمستان سال ۱۴۰۳ بین ۲۵ خبره منتخب (دارای تحصیلات مرتبط و دست‌کم ۱۰ سال سابقه فعالیت پژوهشی و اجرایی) که بصورت هدفمند انتخاب شدند، توزیع شد.

---

[1] Theoretical Saturation
[2] Attride-Stirling
[3] Brooks
[4] Aria

گام ۲: از خبرگان خواسته شد که اهمیت هر یک از مولفه‌های توانمندی فناورانه امنیت سایبری را با استفاده از متغیرهای زبانی تعیین کنند. متغیرهای زبانی و مقیاس‌های فازی متناظر آنها (اعداد فازی مثلثی) برای تعیین اهمیت مولفه‌های توانمندی فناورانه امنیت سایبری در جدول ۱ نشان داده شده است.

جدول ۱: متغیرهای زبانی برای اهمیت مولفه‌های توانمندی فناورانه امنیت سایبری

متغیرهای زبانی	مقیاس فازی
خیلی کم‌اهمیت (VU)	(0,0,0.1)
نسبتا کم‌اهمیت (MU)	(0,0.1,0.3)
کم اهمیت (UN)	(0.1,0.3,0.5)
با اهمیت متوسط (F)	(0.3,0.5,0.7)
با اهمیت (IM)	(0.5,0.7,0.9)
نسبتا با اهمیت (MI)	(0.7,0.9,1)
خیلی با اهمیت (VI)	(0.9,1,1)

برای محاسبهٔ اعداد فازی ($\tilde{a}_i$)، دیدگاه‌های هر خبره بطور مستقیم مد نظر قرار گرفته‌اند. متغیرهای زبانی براساس توابع عضویت مثلثی به اعداد فازی مثلثی تبدیل و بصورت زیر تعریف شدند (آریا و همکاران، ۲۰۲۰):

$$\tilde{a}_i = (a_i, \delta_i, \gamma_i) \quad (۱)$$

گام ۳: برای تجمیع نظرهای خبرگان از میانگین حسابی اعداد فازی مثلثی (چن[1]، ۲۰۰۰) استفاده شد.

$$a_i = \frac{\sum_{k=1}^{n} \beta_{ik}}{N} \rightarrow k = 1, 2, 3, \dots, n \quad (۲)$$

$$\delta_i = \frac{\sum_{k=1}^{n} \beta_{ik}}{N} \rightarrow k = 1, 2, 3, \dots, n \quad (۳)$$

$$\gamma_i = \frac{\sum_{k=1}^{n} \beta_{ik}}{N} \rightarrow k = 1, 2, 3, \dots, n \quad (۴)$$

در روابط فوق، β_{ik} نشان‌دهندهٔ اهمیت نسبی پارمتر i از دیدگاه خبره k ام، γ_i و a_j به ترتیب حد بالا و پایین نظرهای پرسش‌شوندگان و δ_{ij} میانگین نظرهای پرسش‌شوندگان می‌باشد. بدیهی است که مولفه‌های عدد فازی به گونه‌ای تعریف شده‌اند که: $a_{ij} \leq \delta_{ij} \leq \gamma_{ij}$ باشد. در ضمن مقادیر این مؤلفه‌ها در بازه $\left[\frac{1}{9}, 9\right]$ تغییر می‌کنند.

گام ۴: طبق نظر چنگ و لین[2] (۲۰۰۲)، از روش رأسی[3] برای محاسبه فاصله بین ارزیابی هر خبره و میانگین وزنی نظرات استفاده شد. اگر این فاصله کمتر از حد آستانه ۰/۲ باشد، اجماع حاصل شده است و روند دورهای دلفی پایان می‌یابد، درغیراین‌صورت دورهای بعدی دلفی باید اجرا شود.

[1] Chen
[2] Cheng & Lin
[3] Vertex

$$d(\tilde{a}_{i1}, \check{a}_{i2}) = \sqrt{1/6\,[(\alpha_{i1} - \alpha_{i2})^2 + 4(\delta_{i1} - \delta_{i2})^2 + (\gamma_{i1} - \gamma_{i2})^2]} \quad (۵)$$

گام ۵: از روش بهترین عملکرد نافازی‌سازی (BNP) برای قطعی‌سازی استفاده شد.

$$BNP = \frac{(\gamma_i - \alpha_i) + (\delta_i - \alpha_i)}{3} + \alpha_i \quad (۶)$$

گام ۶: میانگین وزن کل عوامل محاسبه و اگر وزن نهایی هر مولفه کمتر از میانگین وزن کل عوامل بود، آن مولفه رد شده، درغیراین‌صورت تایید می‌شود. گراف ۱ روند اجرای مراحل و گام‌های پژوهش را بطور خلاصه نشان می‌دهد.

یافته‌ها

برای شناخت عوامل کلیدی ارتقای توانمندی فناورانه امنیت سایبری در بالادست صنعت نفت و گاز، پیشینه و ادبیات امنیت سایبری و توانمندی فناوری اطلاعات براساس دیدگاه منبع‌محور و داده‌های مصاحبه‌های نیمه‌ساختاریافته تخصصی با بکارگیری رویکرد تحلیل مضمون مطابق مراحل زیر تحلیل شده‌اند: «تولید کدهای اولیه»، «گروه‌بندی کدهای مشابه»، «بررسی و پالایش مضمون‌های سازمان‌دهنده»، «شناسایی مضمون‌های پایه» و «تجدید نظر و بازنگری».

جدول ۲: عوامل کلیدی ارتقاء توانمندی امنیت سایبری در شرکت‌های خدمات‌دهنده نفت و گاز

مضامین سازمان‌دهنده	مضامین پایه	مولف	فراوانی در مصاحبه‌ها
توانمندی منابع‌انسانی	مهارت و شایستگی تیم امنیت	Maarop et al., 2015; Tisdale, 2016 Yeoh et al., 2022	۸
	مسئولیت‌پذیری و تعهد تیم امنیت	Aksoy, 2023	۱۰
	دانش و آگاهی کارکنان	Alnatheer, 2015; Bobbert and Mulder, 2015; Maarop et al., 2015; Yeoh et al., 2022; Aksoy, 2023	۷
	مسئولیت‌پذیری و تعهد کارکنان	-	۵
توانمندی فرایندهای سازمانی	بروزرسانی اطلاعات و آموزش پیوسته تیم امنیت	-	۸
	تهیه و اجرای طرح‌های تداوم کسب و کار	-	۹
	آموزش و اطلاع‌رسانی به کارکنان درباره مسائل امنیت سایبری	Henrie, 2013; Kirova and Baumoel, 2018; Yeoh et al., 2022	-
	اجرای برنامه‌های آموزشی و آگاهی‌بخشی امنیت سایبری	-	۸
	توسعه فرهنگ ارتباطات و همکاری داخلی	Aksoy, 2023	۶
	زیرساخت‌های فنی سخت و نرم	-	۵
	تهیه و بروزرسانی روال‌ها و راهنماها (گایدلاین‌ها)	-	۵

توانمندی فنی و زیرساختی	شناسایی، تجزیه و تحلیل، پیشگیری، پاسخ حملات سایبری	Bobbert and Mulder, 2015; Soomro et al., 2016; Tisdale, 2016; AlGhamdi et al., 2020; Diesch et al., 2020; Yeoh et al., 2022	۴
	بررسی، ممیزی، اندازه‌گیری عملکرد سایبری	-	۷
	گزارش‌گیری و ارزیابی منظم خطرات امنیت سایبری	Sadeghi, 2016; Diesch et al., 2020; Hussain et al., 2020; Yeoh et al., 2022	۷
	آماده‌سازی و آزمایش برنامه‌های واکنش به حوادث سایبری	-	۸
	توسعه و اجرای طرح‌های واکنش به حوادث سایبری	Aksoy, 2023	۵
	تهیه و بکارگیری برنامه‌های کاربردی امنیت شبکه	-	۶
	تهیه و اجرای طرح‌ها و برنامه‌های امنیت شبکه	-	۷
	پشتیبانی امنیت پایگاه داده	-	۶
	تهیه و بکارگیری ابزارهای امنیت شبکه	-	۷
توانمندی راهبردی و مدیریتی	تدوین و تطبیق راهبردهای کسب و کار با ملاحظات امنیتی	Bayuk and Mostashari, 2011; Henrie, 2013; Atkins and Lawson, 2021; Yeoh et al., 2022	۸
	پشتیبانی و انگیزه مدیریت ارشد	-	۷
	سیاست‌های امنیت و استانداردها	-	۶
	ایجاد سیاست‌ای امنیت سایبری	Aksoy, 2023	۶
	اجرای برنامه‌های آموزشی امنیت سایبری	-	۸
	اجرای راهبردها و درنظرگرفتن عامل‌های انسانی	-	۸
	اطمینان از مدیریت موثر امنیت سایبری	-	۷
	رویکرد کل‌نگر (توسعه، تداوم و اجرای راهبردها)	-	۶
	اختصاص بودجه برای امنیت	-	۸
	تعیین اهداف و قوانین و مقررات امنیت سایبری	Aksoy, 2023	-
	مدیریت عامل‌های انسانی	-	۷
توانمندی امنیت	خدمات‌دهندگان 3rd party	Henrie, 2013; Kirova and Baumoel, 2018; Yeoh et al., 2022	۹
	شرکای معاملاتی	Aksoy, 2023	۸

ذی‌نفعان کلیدی	بالادست و پایین دست زنجیره تامین	Maarop et al., 2015; Pandey et al., 2020; Atkins and Lawson, 2022; Yeoh et al., 2022	۱۰
	نهادهای نظارتی	Maarop et al., 2015; Pandey et al., 2020; Atkins and Lawson, 2021; Yeoh et al., 2022	۹
	همکاران	Yeoh et al., 2022; Aksoy, 2023	۷

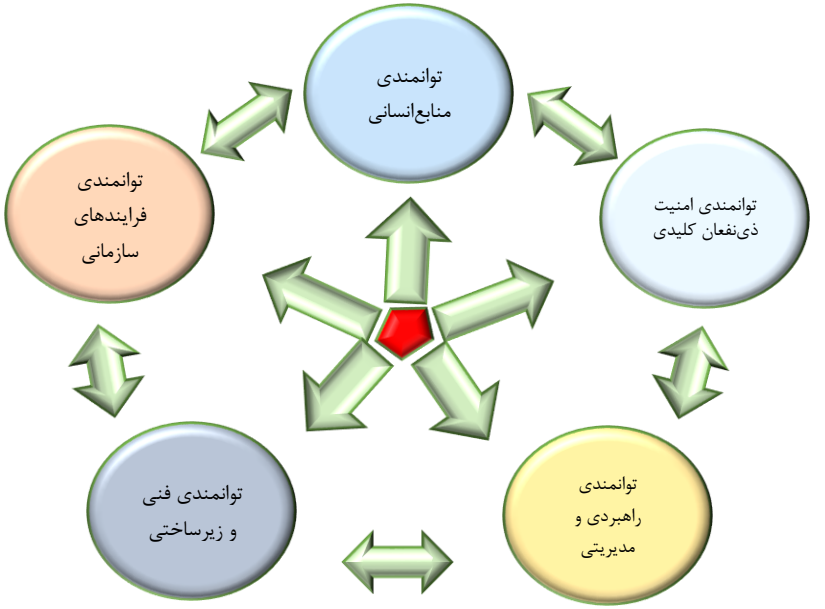
با بررسی پیشینه و ادبیات توانمندی فناوری اطلاعات در دیدگاه منبع‌محور و امنیت سایبری، عوامل کلیدی ارتقاء استخراج شده است. توانمندی فناوری اطلاعات که از صنعت اتخاذ می‌شود، نشان می‌دهد توانمندی فناوری اطلاعات از چهار بعد راهبردهای فناوری اطلاعات، فرآیندهای فناوری اطلاعات، سازمان فناوری اطلاعات (مهارت‌ها، ساختار و دانش/دانش چگونگی) و دارایی/زیرساخت فناوری اطلاعات (سخت‌افزار، نرم‌افزار، برنامه‌های کاربردی، شبکه، پایگاه داده و ابزار) تشکیل شده است. ابعاد مذکور هم توانمندی فنی فناوری اطلاعات (یعنی دارایی‌ها و زیرساخت فناوری اطلاعات) و هم توانمندی‌های مدیریتی را دربرمی‌گیرند که جنبه‌های مختلف مدیریت فناوری اطلاعات از جمله راهبرد، فرآیند و سازمان را پوشش می‌دهد. دیدگاه منبع‌محور توانمندی یک سازمان را ترکیبی می‌داند. یک سازمان از طریق توانمندی فناوری اطلاعات با استفاده از پیکربندی منحصربه‌فرد و ترکیبی از این ابعاد، مانند توانمندی برنامه‌ریزی راهبردی فناوری اطلاعات، توانمندی عملیاتی فناوری اطلاعات (یعنی فرآیند)، توانمندی سازمان فناوری اطلاعات و زیرساخت‌ها و دارایی‌های فناوری اطلاعات، ارزش ایجاد می‌کند. ابعاد توانمندی فناوری اطلاعات، به طبقه‌بندی و تجزیه‌وتحلیل عوامل کلیدی موفقیت امنیت سایبری منجر می‌شود، که درواقع، منابعی هستند که شرکت‌ها هنگام برخورد با امنیت سایبری روی آنها سرمایه‌گذاری کرده یا ساخته‌اند، و چنین منابعی برای کمک به سازمان برای از بین بردن تهدیدهای بالقوه فضای مجازی یکپارچه می‌شوند. درنهایت، با بررسی پیشینه و ادبیات توانمندی فناوری اطلاعات براساس دیدگاه منبع‌محور و امنیت سایبری، ۱۶ عامل کلیدی (مضمون پایه) از منابع گوناگون برای ارتقای توانمندی امنیت سایبری استخراج شده است. درادامه، در ترکیب مضامین مستخرج از پیشینه و ادبیات پژوهش با تحلیل مصاحبه‌های خبرگان از طریق رویکرد تحلیل مضمون، عوامل کلیدی ارتقای توانمندی فناورانه امنیت سایبری در بالادست صنعت نفت و گاز در ۵ مضمون سازمان‌دهنده و ۳۶ مضمون پایه شناسایی و دسته‌بندی شدند. مضامین سازمان‌دهنده شامل توانمندی منابع‌انسانی با ۴ مضمون پایه، توانمندی فرایندهای سازمانی با ۵ مضمون پایه، توانمندی فنی و زیرساختی امنیتی با ۱۱ مضمون پایه، توانمندی راهبردی و مدیریتی با ۱۱ مضمون پایه، توانمندی امنیتی ذی‌نفعان کلیدی با ۵ مضمون پایه تشکیل شده است. سپس، با انجام دلفی فازی عامل‌های کلیدی ارتقاء توانمندی امنیت سایبری در بالادست صنعت نفت و گاز تصحیح و غربالگری شدند. تجمیع نتایج تحلیل مضمون مصاحبه‌ها و دلفی فازی در جدول ۳ ارائه شده است.

جدول ۳: عوامل کلیدی ارتقاء توانمندی امنیت سایبری در شرکت‌های خدمات‌دهنده نفت و گاز

مضامین سازمان دهنده	مضامین پایه	میانگین فازی دور نخست	میانگین فازی دور دوم	میانگین قطعی دور دوم	وضعیت
توانمندی منابع انسانی	مهارت و شایستگی تیم امنیت	(0.716,0.88,0.712)	(0.788,0.944,0.944)	0.8920	پذیرش
	مسئولیت‌پذیری و تعهد تیم امنیت	(0.66,0.832,0.544)	(0.796,0.948,0.948)	0.8973	پذیرش
	دانش و آگاهی کارکنان	(0.668,0.848,0.632)	(0.804,0.952,0.952)	0.9027	پذیرش
	مسئولیت‌پذیری و تعهد کارکنان	(0.724,0.888,0.744)	(0.788,0.944,0.944)	0.8920	پذیرش
توانمندی فرآیندهای سازمانی	بروزرسانی اطلاعات و آموزش پیوسته تیم امنیت	(0.732,0.888,0.72)	(0.804,0.952,0.952)	0.9027	پذیرش
	تهیه و اجرای طرح‌های تداوم کسب و کار	(0.356,0.556,0.716)	(0.396,0.596,0.516)	0.5027	حذف
	آموزش و اطلاع‌رسانی به کارکنان درباره مسائل امنیت سایبری	(0.396,0.596,0.652)	(0.38,0.58,0.58)	0.5133	ادغام
	اجرای برنامه‌های آموزشی و آگاهی‌بخشی کارکنان درباره امنیت سایبری	(0.74,0.904,0.808)	(0.788,0.944,0.944)	0.8920	پذیرش
	توسعه فرهنگ ارتباطات و همکاری داخلی	(0.74,0.904,0.808)	(0.796,0.948,0.948)	0.8973	پذیرش
توانمندی فنی و زیرساختی	زیرساخت‌های فنی سخت و نرم	(0.836,0.96,0.912)	(0.78,0.908,0.78)	0.8227	پذیرش
	تهیه و بروزرسانی روال‌ها و راهنماها (گایدلاین‌ها)	(0.668,0.844,0.604)	(0.788,0.944,0.944)	0.8920	پذیرش
	شناسایی، تجزیه و تحلیل، پیشگیری، پاسخ حملات سایبری	(0.292,0.492,0.62)	(0.38,0.58,0.58)	0.5133	ادغام
	بررسی، ممیزی، اندازه‌گیری عملکرد امنیت سایبری	(0.7,0.864,0.648)	(0.788,0.944,0.944)	0.8920	پذیرش
	گزارش‌گیری و ارزیابی منظم خطرات امنیت سایبری	(0.74,0.904,0.808)	(0.788,0.916,0.748)	0.8173	پذیرش
	آماده‌سازی و آزمایش برنامه‌های واکنش به حوادث و حملات سایبری	(0.74,0.904,0.808)	(0.74,0.872,0.84)	0.8173	پذیرش
	توسعه و اجرای طرح‌های واکنش به حوادث و حملات سایبری	(0.692,0.868,0.7)	(0.788,0.944,0.944)	0.8920	پذیرش
	تهیه و بکارگیری برنامه‌های کاربردی امنیت شبکه	(0.3,0.5,0.684)	(0.452,0.652,0.292)	0.4653	ادغام
	تهیه و اجرای طرح‌ها و برنامه‌های امنیت شبکه	(0.668,0.848,0.632)	(0.764,0.896,0.744)	0.8013	پذیرش
	پشتیبانی امنیت پایگاه داده	(0.676,0.856,0.664)	(0.812,0.956,0.956)	0.9080	پذیرش
	تهیه و بکارگیری ابزارهای امنیت شبکه	(0.668,0.848,0.632)	(0.804,0.928,0.784)	0.8387	پذیرش
توانمندی راهبردی و مدیریتی	تدوین و تطبیق راهبردهای کسب و کار با ملاحظات امنیتی	(0.74,0.908,0.836)	(0.788,0.944,0.944)	0.8920	پذیرش
	سیاست‌های امنیت و استانداردها	(0.316,0.516,0.708)	(0.444,0.644,0.324)	0.4707	ادغام
	پشتیبانی و اطمینان از مدیریت موثر امنیت سایبری	(0.772,0.912,0.768)	(0.796,0.948,0.948)	0.8973	پذیرش
	ایجاد سیاست‌های امنیت سایبری	(0.236,0.436,0.716)	(0.388,0.584,0.592)	0.5213	ادغام
	رویکرد کل‌نگر (توسعه، تداوم و اجرای راهبردها)	(0.724,0.892,0.772)	(0.788,0.944,0.944)	0.8920	پذیرش
	اجرای راهبردها و درنظرگرفتن عوامل انسانی	(0.7,0.872,0.704)	(0.788,0.944,0.944)	0.8920	پذیرش
	پشتیبانی و انگیزه مدیریت ارشد	(0.348,0.548,0.62)	(0.388,0.588,0.548)	0.5080	ادغام
	اجرای برنامه‌های آموزشی امنیت سایبری	(0.26,0.46,0.708)	(0.364,0.564,0.644)	0.5240	ادغام
	مدیریت عوامل‌انسانی	(0.332,0.532,0.516)	(0.372,0.572,0.612)	0.5187	ادغام
	اختصاص بودجه برای امنیت	(0.724,0.896,0.8)	(0.788,0.944,0.944)	0.8920	پذیرش

	تعیین اهداف و قوانین و مقررات امنیت سایبری	(0.74,0.912,0.864)	(0.788,0.944,0.944)	0.8920	پذیرش
توانمندی امنیت ذی‌نفعان کلیدی	کیفیت ارتباط متقابل با خدمات‌دهندگان فرعی[1]	(0.636,0.82,0.532)	(0.788,0.944,0.944)	0.8920	پذیرش
	مدیریت حجم و پیچیدگی اطلاعات بین شرکای داخلی	(0.684,0.856,0.64)	(0.788,0.944,0.944)	0.8920	پذیرش
	قابلیت اعتماد در بالادست و پایین‌دست زنجیره‌تأمین	(0.7,0.88,0.76)	(0.788,0.944,0.944)	0.8920	پذیرش
	سیاست‌های امنیتی و پشتیبانی نهادهای نظارتی	(0.756,0.912,0.816)	(0.796,0.948,0.948)	0.8973	پذیرش
	ایمن‌سازی شبکه‌های تبادل اطلاعات با همکاران خارجی	(0.732,0.908,0.86)	(0.788,0.944,0.944)	0.8920	پذیرش

در ادامه، رویکرد دلفی فازی برای تعیین اهمیت نسبی معیارهای مستخرج از بخش قبل بکار گرفته شد. از این‌رو، پرسشنامه‌ای با طیف لیکرت ۹ گزینه‌ای با ۳۶ سوال (هر سوال بیانگر یک عامل) طراحی و توسط خبرگان تکمیل گردید. با اجرای دو دور دلفی و با توجه به این که فاصله رأسی بین ارزیابی هر خبره و میانگین وزنی نظرات خبرگان در دور دوم کمتر از حد آستانه ۰/۲ گردید، بنابراین، در دور دوم اجماع حاصل شده است. درنتیجه، برای تعیین وضعیت هر عامل، میانگین قطعی وزن کل عوامل در دور دوم محاسبه و اگر وزن نهایی هر عامل کمتر از میانگین وزن کل عوامل بود، آن مولفه رد، درغیراین‌صورت تأیید شده است. درنهایت، مدل عوامل کلیدی ارتقای توانمندی فناورانه امنیت سایبری در شرکت‌های خدمات‌دهنده بالادست نفت و گاز ترسیم شده است.



شکل ۱: عوامل کلیدی ارتقاء توانمندی فناورانه امنیت سایبری در شرکت‌های خدمات‌دهنده بالادست نفت و گاز

[1] 3rd Party

بدین‌ترتیب، ۹ عامل کلیدی شامل عامل‌های «تهیه و اجرای طرح‌های تداوم کسب و کار»، «آموزش و اطلاع‌رسانی به کارکنان درباره مسائل امنیت سایبری»، «شناسایی، تجزیه و تحلیل، پیشگیری، پاسخ حملات سایبری»، «تهیه و بکارگیری برنامه‌های کاربردی امنیت شبکه»، «سیاست‌های امنیت و استانداردها»، «ایجاد سیاست‌های امنیت سایبری»، «پشتیبانی و انگیزه مدیریت ارشد»، «اجرای برنامه‌های آموزشی امنیت سایبری» و «مدیریت عوامل انسانی» به دلیل تکراری بودن یا ادغام با سایر عوامل از مجموعه عوامل کلیدی توانمندی امنیت سایبری حذف گردیدند و درنهایت، ۲۷ مضمون پایه یا عامل کلیدی تایید شد. در نتیجه مضامین سازمان‌دهنده شامل توانمندی منابع‌انسانی با ۴ مضمون پایه، توانمندی فرایندهای سازمانی با ۳ مضمون پایه، توانمندی فنی و زیرساختی امنیتی با ۹ مضمون پایه، توانمندی راهبردی و مدیریتی با ۶ مضمون پایه، توانمندی امنیتی ذی‌نفعان کلیدی با ۵ مضمون پایه تشکیل شده است.

بحث و نتیجه‌گیری

امنیت سایبری یک جنبه حیاتی از امنیت اجتماعی و سازمانی است و نقش اساسی در دستیابی به اهداف راهبردی یک سازمان در یک جامعه دیجیتالی ایفا می‌کند. در دهه اخیر، حملات سایبری به زیرساخت‌های حیاتی کشور ایران تکرار شده است که نگرانی درباره احتمال وقوع مجدد تهدیدات هدفمند سایبری علیه این زیرساخت‌ها را افزایش داده است. بنابراین، ارتقای توانمندی‌های فناورانه امنیت سایبری زیرساخت‌های حیاتی بویژه در بالادست صنعت نفت و گاز از اهمیت بالایی برخوردار است. زیرا با توجه به وابستگی قابل‌توجه تولید ناخالص داخلی ایران به بالادست صنعت نفت و گاز و صنایع مرتبط به آن؛ آسیب به زیرساخت‌های این صنعت می‌تواند به صورت آبشاری سبب حوادث گسترده‌ای در شبکه زیرساخت‌های مرتبط شود. این تهدیدها می‌تواند توسط کارکنان ناراضی، جاسوسان صنعتی، سازمان‌های اطلاعاتی یا ارتش‌های سایبری صورت گیرد. از این جهت، در مقاله حاضر به شناسایی عوامل کلیدی ارتقای توانمندی‌های فناورانه امنیت سایبری زیرساخت‌های حیاتی با تأکید بر بالادست صنعت نفت و گاز پرداخته شده است.

مدیریت امنیت سایبری شامل توانمندسازی کسب‌وکارها برای فعالیت بر روی شبکه‌های اطلاعاتی، با هدف اصلی حصول اطمینان از مشارکت همه ذی‌نفعان در ایجاد یک سیستم امنیت سایبری قوی است. در زمینه کارکنان نکته مهم بکارگیری نیروی انسانی متعهد و آموزش‌دیده است که از شیوه‌های نهدید آگاهی کامل داشته باشند. بنابراین، یکی از اهداف مدیریت امنیت سایبری شناسایی و جلوگیری از حملات سایبری با اتخاذ تقویت آگاهی امنیت اطلاعات کارکنان از طریق آموزش است. اما برای رسیدن به این هدف، آموزش کارکنان کافی نیست، درعین‌حال باید رفتارهای ایمن کارکنان را تشویق کرد و در سراسر سازمان گسترش داد. این زمانی اتفاق می‌افتد که بالادست صنعت نفت و گاز فرهنگ ایمنی را اتخاذ کنند. اتخاذ فرهنگ امنیتی در بالادست صنعت نفت و گاز، افزایش آگاهی کارکنان در زمینه امنیت سایبری، ارائه آموزش و اطلاعات در زمینه امنیت سایبری، تعیین و اجرای سیاست‌های امنیت سایبری، نظارت و ارزیابی مستمر امنیت سایبری سیستم‌های اطلاعاتی، تهیه و طرح‌های واکنش به حوادث سایبری. همچنین، در این زمینه

وجود پروتکل‌های احراز هویت و مجوزهای اختیارات و حسابرسی می‌تواند به تعیین سطح دسترسی، حفظ محرمانگیو یکپارچگی کمک شایانی نماید.

مشارکت تعداد زیادی از خدمات‌دهندگان فرعی، حجم و تبادل اطلاعات بین شرکای داخلی و خارجی در بالادست صنعت نفت و گاز نیز می‌تواند موجب افشای اطلاعات زیرساخت‌ها، تشخیص نقاط ضعف ذاتی و آسیب‌پذیری شود. بنابراین، چگونگی روابط و تعامل بازیگران داخلی و شرکای خارجی در مقابله با حملات سایبری از اهمیت بالایی برخوردار است. ادغام فعالیت‌هایی مانند همکاری با همه ذینفعان درباره موضوع و نظارت مستمر خطرات امنیت سایبری در فرهنگ سازمانی با مشارکت همه کارکنان بویژه مدیریت الزامی است. همچنین، کیفیت ارتباط متقابل با خدمات‌دهندگان فرعی، مدیریت حجم و پیچیدگی اطلاعات بین شرکای داخلی، قابلیت اعتماد در بالادست و پایین‌دست زنجیره‌تأمین، سیاست‌های امنیتی و پشتیبانی نهادهای نظارتی و ایمن‌سازی شبکه‌های تبادل اطلاعات با همکاران خارجی در این زمینه می‌تواند بسیار مفید باشد.

محدودیت‌ها و پیشنهادها

برای دستیابی به امنیت سایبری و مدیریت اثربخش آن نه تنها به کنترل‌های فنی همه‌جانبه نیاز است، بلکه مدیریت عوامل انسانی نیز از اهمیت بسیار بالایی برخوردار است. علاوه بر تضمین امنیت سیستم‌های کنترل فنی، افراد نیز نقش مهمی در مدیریت امنیت سایبری ایفاء می‌کنند. بنابراین، توصیه می‌شود شرکت‌های فعال در بالادست نفت و گاز رویکردی جامع که همه جنبه‌های امنیت سایبری یعنی به لحاظ راهبردی، فنی و زیرساختی، مدیریتی، منابع انسانی و ذی‌نفعان کلیدی را دربر می‌گیرد، برای مدیریت امنیت سایبری اتخاذ کنند.

برای اطمینان از امنیت سایبری، برای شرکت‌های فعال در بالادست نفت و گاز پیشنهاد می‌شود که دانش، آگاهی و مهارت‌های خود را از طریق آموزش و برنامه‌های آگاه‌سازی و استخدام تیم امنیت قوی افزایش دهند. زیرا آگاهی، دانش معتبر و بروزرسانی شده به کارمندان امکان می‌دهد که درباره تهدیدات سایبری بالقوه مطلع باشند و مهارت‌های خود را برای مقابله با چنین خطراتی توسعه داده و توانایی آنها برای شناسایی و گزارش حملات سایبری افزایش یابد. بنابراین، توصیه می‌شود شرکت‌های فعال در بالادست صنعت نفت و گاز آگاهی و دانش مدیران و کارکنان خود درباره امنیت سایبری را از طریق تدوین برنامه‌های آموزشی مناسب و پرورش فرهنگ امنیت سایبری افزایش دهند.

مدیریت امنیت سایبری فراتر از فناوری است و با مدیریت افراد، رفتار سازمانی، یادگیری مستمر، فرهنگ سازمانی و تغییر پیوندهای داخلی و خارجی ارتباط تنگاتنگی دارد. مدیریت امنیت سایبری چگونگی درک کارکنان از امنیت سایبری و اولویت‌ها و اقدامات آنها، تحت تأثیر باورها، ارزش‌ها و نگرش‌های هر یک از آنها (از هیأت مدیره گرفته تا هر گوشه از شرکت‌های فعال در بالادست صنعت نفت و گاز) است. بنابراین، به مدیران فعال در این حوزه توصیه می‌شود تا با پشتیبانی و اطمینان از مدیریت موثر امنیت سایبری و رویکرد کل‌نگر (توسعه، تداوم و اجرای راهبردها) و همچنین، اختصاص بودجه برای امنیت و تعیین اهداف و قوانین و مقررات امنیت سایبری به ارتقای توانمندی کمک نمایند.

پیشنهاد می‌شود شرکت‌های فعال در بالادست صنعت نفت و گاز بطور پیوسته کارکنان خود را در زمینه امنیت سایبری آموزش دهند، زیرا بسیاری از حملات سایبری به دلیل بی‌دقتی یا ناآگاهی کارکنان رخ می‌دهد. افزایش آگاهی از امنیت سایبری بستگی به این دارد که شرکت‌های بالادست نفت و گاز برنامه‌های آموزشی مناسب درباره امنیت سایبری را توسعه دهند. برنامه‌های آموزشی امنیت سایبری شرکت‌های بالادست نفت و گاز برای آگاهی کارکنان از امنیت سایبری طراحی شده است. این برنامه‌ها کارمندان را قادر می‌سازد مفاهیم امنیت سایبری، تهدیدات، خطرات، حملات، روش‌های حفاظتی و روش‌های گزارش‌دهی را درک کنند. علاوه‌براین، توصیه می‌شود برنامه‌های آموزشی باید بطور مرتب توسط شرکت‌های بالادست نفت و گاز تجدید و بروز شوند. این برنامه‌ها کارکنان را قادر می‌سازد تا آگاهانه از تهدیدات فعلی امنیت سایبری جلوگیری کرده و از روش‌های محافظت در برابر حملات مطلع شوند.

منابع

اختری، محمد، کرامتی، محمدعلی، و موسوی، سیدعبدالهامین. (۱۴۰۲الف). ارائه مدل مفهومی بلوغ امنیت سایبری برای زیرساختهای حیاتی کشور. *آینده پژوهی دفاعی*، *۱*(۲۰)، ۱۹۱-۱۳۴.

اختری، محمد، کرامتی، محمدعلی، و موسوی، سیدعبدالهامین. (۱۴۰۲ب). ارائه مدل بلوغ امنیت سایبری برای زیرساختهای حیاتی. *رشد فناوری*، ۲(۷۵)، ۳۲-۲۲.

بهی فر, مریم, رضوی, محمدرضا. و جعفری, پریوش. (۱۴۰۲). شناسایی توانمندی‌های فناورانه ژئومکانیک در صنعت نفت و گاز. *نشریه علمی ژئومکانیک نفت*، *۶* (۲) ۶۳-۴۸.

بیگزاده، ابراهیم. (۱۴۰۴). تعرض به زیرساخت های حیاتی و حقوق بین الملل. *فصلنامه تحقیقات حقوقی*, *۲۸*(۴), ۳-۲۲. https://doi.org/10.48308/jlr.2025.241688.2965

کافی، سعید. (۱۳۹۹). شاخص‌های دفاعی امنیتی فضای سایبری زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران مبتنی‌بر رویکردهای پدافند غیرعامل. سیاست دفاعی، ۲۸ (۱۱۱)، SID. https://sid.ir/paper/525941/fa

صولت رفیعی، ابوذر، قرائی گرگانی، حسین، ثقفی، فاطمه، و ملکی‌نیا، محمد. (۱۴۰۳). ارتباط، اهمیت و وابستگی زیرساخت های حیاتی جمهوری اسلامی ایران از منظر سایبری. *فناوری اطلاعات و ارتباطات ایران*، ۲(۶۱-۶۲)، ۲۶۱-۲۸۱.

نعمت پور, اردشیر, تقی‌زاده انصاری، مصطفی، و ببری گنبدی، سکینه. (۱۴۰۰). مقابله با حملات تروریستی به زیرساخت های حیاتی یک کشور در قواعدحقوق بین الملل. *فصلنامه مطالعات بین المللی*, *۱۸*(۳), ۱۶۵-۱۸۵. https://doi.org/10.22034/isj.2022.301984.1573

واعظی‌نژاد محمد مهدی، و مقدس محمدرضا، (۱۳۹۴) ، راهبردهای امن‌سازی زیرساخت‌های حیاتی کشور در حوزه فناوری اطلاعات، کتاب الکترونیک، mvaezi.ir

Aksoy, C. (2023). Critical success factors for cybersecurity just technical? Exploring the role of human factors in cybersecurity management. *Research Journal of Business and Management*, *10*(2), 51-57. https://doi.org/10.17261/Pressacademia.2023.1735

Aksoy, C. (2024). Building a cyber security culture for resilient organizations against cyber attacks. İşletme Ekonomi ve Yönetim Araştırmaları Dergisi, *7*(1), 96-110. https://doi.org/10.33416/baybem.1374001

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & security*, *99*, 102030.

Alnatheer, M. A., (2015). Information security culture critical success factors. In12th International Conference on Information Technology: New Generations, ITNG 2015, pp. 731–735, Las Vegas, NV, USA. https://doi.org/10.1109/ITNG.2015.124

Aria, A., Jafari, P., & Behifar, M. (2020). The Impediments to Student Engagement: A Hybrid Method Based on Fuzzy Delphi and Fuzzy DEMATEL. *World Journal of Education*, *10*(5), 45-60. https://doi.org/10.5430/wje.v10n5p45

Atkins, S., & Lawson, C. (2022). Integration of effort: Securing critical infrastructure from cyberattack. Public Administration Review, 82(4), 771-775. https://doi.org/10.1111/puar.13493

Attride-Stirling, J. (2001). Thematic networks: an analytic tool for qualitative research. *Qualitative research*, *1*(3), 385-405. https://doi.org/10.1177/146879410100100307

Baikloy, E., Praneetpolgrang, P., & Jirawichitchai, N. (2020). Development of Cyber Resilient Capability Maturity Model for Cloud Computing Services. *TEM Journal*, *9*(3), 915–923.

Bajpai, S., & Gupta, J. P. (2007). Securing oil and gas infrastructure. *Journal of Petroleum Science and Engineering*, *55*(1-2), 174-186. https://doi.org/10.1016/j.petrol.2006.04.007

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of management*, *17*(1), 99-120. https://doi.org/10.1177/014920639101700108

Barney, J. B. (2001). Resource-based theories of competitive advantage: A ten-year retrospective on the resource-based view. *Journal of management*, *27*(6), 643-650. https://doi.org/10.1177/014920630102700602

Bayuk, J. L., & Mostashari, A. (2011, November). Measuring cyber security in intelligent urban infrastructure systems. In 2011 8th International Conference & Expo on Emerging Technologies for a Smarter World (pp. 1-6). IEEE. 10.1109/CEWIT.2011.6135873

Becker, M. C. (2004). Organizational routines: a review of the literature. *Industrial and corporate change*, *13*(4), 643-678. https://doi.org/10.1093/icc/dth026

Berndt, A., & Ophoff, J. (2020). Exploring the value of a cyber threat intelligence function in an organization. In *IFIP World Conference on Information Security Education* (pp. 96-109). Cham: Springer International Publishing.

Bharadwaj, A. S., (2000). A resource-based perspective on information technology capability and firm performance: an empirical investigation. *MIS Quarterly, 24*(1),

169–196. https://doi.org/10.2307/3250983

Bhatt, G. D., & Grover, V. (2005). Types of information technology capabilities and their role in competitive advantage: An empirical study. *Journal of management information systems*, *22*(2), 253-277.

Bobbert, Y., & Mulder, H. (2015, December). Governance practices and critical success factors suitable for business information security. In 2015 International Conference on Computational Intelligence and Communication Networks (CICN) (pp. 1097-1104). IEEE. 10.1109/CICN.2015.216

Brooks, J., Horrocks, C., & King, N. (2018). Interviews in qualitative research. *Interviews in qualitative research*, 1-360.

Chakravarty, A., Grewal, R., & Sambamurthy, V. (2013). Information technology competencies, organizational agility, and firm performance: Enabling and facilitating roles. *Information systems research*, *24*(4), 976-997. https://doi.org/10.1287/isre.2013.0500

Chen, C. T. (2000). Extensions of the TOPSIS for group decision-making under fuzzy environment. *Fuzzy sets and systems*, *114*(1), 1-9. https://doi.org/10.1016/S0165-0114(97)00377-1

Chen, Y., Wang, Y., Nevo, S., Jin, J., Wang, L., & Chow, W. S. (2014). IT capability and organizational performance: the roles of business process agility and environmental factors. *European journal of information systems*, *23*(3), 326-342. https://doi.org/10.1057/ejis.2013.4

Cheng, C. H., & Lin, Y. (2002). Evaluating the best main battle tank using fuzzy decision theory with linguistic criteria evaluation. *European journal of operational research*, *142*(1), 174-186. https://doi.org/10.1016/S0377-2217(01)00280-6

Cordner, L. (2011). Managing regional risk: offshore oil and gas safety and security in the Asia-Pacific region. *Australian Journal of Maritime & Ocean Affairs*, *3*(1), 15-24. https://doi.org/10.1080/18366503.2011.10815672

Creswell, J. W. (2014). *A concise introduction to mixed methods research*. SAGE publications.

CSA. (2021). Cybersecurity - Not Just A Technical Issue. Singapore Government https://www.csa.gov.sg/en/singcert/Publications/ cybersecurity- not- just- a-technical- issue

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, *92*, 101747. https://doi.org/10.1016/j.cose.2020.101747

Eisenhardt, K. M., & Martin, J. A. (2017). Dynamic capabilities: what are they? *The SMS Blackwell handbook of organizational capabilities*, 341-363. https://doi.org/10.1002/9781405164054.ch21

Esterberg, K. G. (2002). *Qualitative Methods in Social Research*. NY, New York: McGraw-Hill.

Felin, T., & Foss, N. J. (2009). Organizational routines and capabilities: Historical drift and a course-correction toward microfoundations. *Scandinavian journal of management*, *25*(2), 157-167. https://doi.org/10.1016/j.scaman.2009.02.003

Fortinet. (May 2023). State of Operational Technology and Cybersecurity Report

Fortinet (October 2023). Cybersecurity in the Oil and Gas Industry: Securing the OT Environment.

Grant, R. M. (1996). Prospering in dynamically-competitive environments: Organizational capability as knowledge integration. *Organization science*, *7*(4), 375-387. https://doi.org/10.1287/orsc.7.4.375

Grant, R. M., & Verona, G. (2015). What's holding back empirical research into organizational capabilities? Remedies for common problems. *Strategic organization*, *13*(1), 61-74. https://doi.org/10.1177/1476127014565988

Gupta, M., & George, J. F. (2016). Toward the development of a big data analytics capability. *Information & management*, *53*(8), 1049-1064. https://doi.org/10.1016/j.im.2016.07.004

Harel, A. (2012). Preventing terrorist attacks on offshore platforms: Do States have sufficient legal tools? *Harvard National Security Journal*, *4*(1), 131.

Henrie, M. (2013). Cyber security risk management in the SCADA critical infrastructure environment. *Engineering Management Journal*, *25*(2), 38-45. https://doi.org/10.1080/10429247.2013.11431973

Hussain, A., Mohamed, A., & Razali, S. (2020). A review on cybersecurity: Challenges & emerging threats. In *Proceedings of the 3rd international conference on networking, information systems & security* (pp. 1-7). https://doi.org/10.1145/3386723.3387847

Iaiani, M., Moreno, V. C., Reniers, G., Tugnoli, A., & Cozzani, V. (2021b). Analysis of events involving the intentional release of hazardous substances from industrial facilities. *Reliability Engineering & System Safety*, *212*, 107593. https://doi.org/10.1016/J.RESS.2021.107593

Iaiani, M., Musayev, N., Tugnoli, A., Macini, P., Cozzani, V., & Mesini, E. (2021a). Analysis of security threats for offshore Oil&gas operations. *Chemical Engineering Transactions*, *86*, 319-324. https://doi.org/10.3303/CET2186054

John, A., Yang, Z., Riahi, R., & Wang, J. (2016). A risk assessment approach to improve the resilience of a seaport system using Bayesian networks. *Ocean Engineering*, *111*, 136-147. https://doi.org/10.1016/J.OCEANENG.2015.10.048

Johnson, C., Feldman, L. & Witte, G. (2017), Cyber Threat Intelligence and Information Sharing, ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=923332

Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. *International Journal of Critical Infrastructure Protection*, *15*, 47-59. https://doi.org/10.1016/j.ijcip.2016.10.001

Karimi, J., Somers, T. M., & Bhattacherjee, A. (2007). The role of information systems resources in ERP capability building and business process outcomes. *Journal of Management Information Systems*, *24*(2), 221-260. https://doi.org/10.2753/MIS0742-1222240209

Kashubsky, M. (2011). A chronology of attacks on and unlawful interferences with, offshore oil and gas installations, 1975–2010. *Perspectives on Terrorism*, *5*(5/6), 139-167. https://www.jstor.org/stable/26298542

Kirova, D., & Baumoel, U. (2018). Factors that affect the success of security education, training, and awareness programs: a literature review. *Journal of Information Technology Theory and Application (JITTA)*, *19*(4), 4. https://aisel.aisnet.org/jitta/vol19/iss4/4

Lu, Y., & Ramamurthy, K. (2011). Understanding the Link Between Information Technology Capability and Organizational Agility: An Empirical Examination1. *MIS quarterly*, *35*(4), 931-954. https://doi.org/10.2307/41409967

Maarop, N., Mustapha, N. M., Yusoff, R., Ibrahim, R., & Zainuddin, N. M. M. (2015). Understanding success factors of an information security management system plan phase self-implementation. *International Journal of Computer and Information Engineering*, *9*(3), 884-889.

Mata, F. J., Fuerst, W. L., & Barney, J. B. (1995). Information technology and sustained competitive advantage: A resource-based analysis. *MIS quarterly*, *19*(4), 487-505. https://doi.org/10.2307/249630

Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Information technology and organizational performance: an integrative model of it business value1. *MIS quarterly*, *28*(2), 283-322. https://doi.org/10.2307/25148636

Meng, X., Sun, B., & Zhu, D. (2021). Harbour protection: moving invasion target interception for multi-AUV based on prediction planning interception method. *Ocean Engineering*, *219*, 108268. https://doi.org/10.1016/J.OCEANENG.2020.108268

Merriam-Webster (2023). Cybersecurity. Merriam-Webster.com Dictionary. https://www.merriam-webster.com/dictionary/cybersecurity

Meszaros, R. (2017). A Digital future for Oil and Gas. s.l.: Accenture. https://s3.amazonaws.com/bizzabo.users.files/27UDMvJRJ6w3WSvUq8j1_BC

Mik-Meyer, N. (2020). Multimethod qualitative research. *Qualitative research*, *5*(1), 357-374.

Mikalef, P., & Gupta, M. (2021). Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. *Information & management*, *58*(3), 103434. https://doi.org/10.1016/j.im.2021.103434

Mohammed, I., & Bade, A. M. (2019). Cybersecurity capability maturity model for network system. *International Journal of Development Research*, *9*(07), 28637-28641.

Pandey, S., Singh, R.K., Gunasekaran, A., Kaushik, A., 2020. Cyber security risks in globalized supply chains: conceptual framework. J. Global Operat. Strat. Sour. *13*(1), 103–128.

Paulk, M. C. (2009). A history of the capability maturity model for software. *ASQ Software Quality Professional, 12*(1), 5–19.

Peteraf, M. A. (1993). The cornerstones of competitive advantage: a resource-based view. *Strategic management journal*, *14*(3), 179-191. https://doi.org/10.1002/smj.4250140303

Progoulakis, I., & Nikitakos, N. (2019). Risk assessment framework for the security of offshore oil and gas assets. In *Proc. IAME 2019 Conf* (pp. 1-25).

PwC. (2021). PwC's 24th Annual Global CEO Survey: CEOs on their tech concerns. 2021 (24 March 2021), Report by PwC annual survey of CEO on IT or technology concerns. (UK based). https://www.pwc.com.au/digitalpulse/ report- pwc- 24th-ceo- survey.html

Sade-Beck, L. (2004). Internet ethnography: Online and offline. *International Journal of Qualitative Methods*, *3*(2), 45-51. https://doi.org/10.1177/160940690400300204

Sadeghi, R. A. (2016). Identifying key success factors in the implementation of information security systems on service businesses: A case study of the private banks of Tehran. American Journal of Theoretical and Applied Business, 2(4), 28-37.

Sandhu, J. S. (2021). *Cybersecurity for executives: Advancing leaders to practical cyber risk management*. Notion Press.

Santhanam, R., & Hartono, E. (2003). Issues in Linking Information Technology Capability to Firm Performance1. *MIS quarterly*, *27*(1), 125-153. https://doi.org/10.2307/30036521

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 8.

Silverman, D. (2019). Interpreting qualitative data. 1-568.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International journal of information management*, *36*(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Steinhäusler, F., Furthner, P., Heidegger, W., Rydell, S., & Zaitseva, L. (2008). Security risks to the oil and gas industry: Terrorist capabilities. *Strategic Insights VII*(1).

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic management journal*, *18*(7), 509-533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7%3C509::AID-SMJ882%3E3.0.CO;2-Z

Tisdale, S. M. (2016). Architecting A cybersecurity managment framework. *Issues in Information Systems*, *17*(4), 227–236. https://doi.org/10.48009/4_iis_2016_227-236

Vasilev, V. S. (2016). Some specifics of reducing the IED risk in offshore securit y environment. *Micea Cel Batran" Nav Acad Sci Bull*, *19*, 116-127.

Wade, M., & Hulland, J. (2004). the resource-based view and information systems research: review, extension, and suggestions for future Research1. *MIS quarterly*, *28*(1), 107-142. https://doi.org/10.2307/25148626

Wang, Z., & Kim, H. G. (2017). Can social media marketing improve customer relationship capabilities and firm performance? Dynamic capability perspective. *Journal of Interactive marketing*, *39*(1), 15-26. https://doi.org/10.1016/j.intmar.2017.02.004

Ware, W. H. (1970). *Security controls for computer systems*. Technical report, Rand Corp Santa Monica, CA, USA.

Yeoh, W., Huang, H., Lee, W. S., Al Jafari, F., & Mansson, R. (2022). Simulated phishing attack and embedded training campaign. *Journal of Computer Information Systems*, *62*(4), 802-821. https://doi.org/10.1080/08874417.2021.1919941

Yoon, C. Y. (2011). Measuring enterprise IT capability: a total IT capability perspective. *Knowledge-Based Systems*, *24*(1), 113-118. https://doi.org/10.1016/j.knosys.2010.07.011

Zhou, X. (2022). A comprehensive framework for assessing navigation risk and deploying maritime emergency resources in the South China Sea. *Ocean Engineering*, *248*, 110797. https://doi.org/10.1016/j.oceaneng.2022.110797

Zhou, X. Y., Liu, Z. J., Wang, F. W., & Wu, Z. L. (2021). A system-theoretic approach to safety and security co-analysis of autonomous ships. *Ocean Engineering*, *222*, 108569. https://doi.org/10.1016/J.OCEANENG.2021.108569

Zhuang, Y., & Lederer, A. L. (2006). A resource-based view of electronic commerce. *Information & management*, *43*(2), 251-261. https://doi.org/10.1016/j.im.2005.06.006

Key factors for improving cybersecurity technological capabilities in critical infrastructure

Maryam Behifar
Phd. Student of Technology Management, SR.C., Islamic Azad University, Tehran, Iran.

Mohammad Reza Razavi*[1]
Assistant Professor, Department of Technology Management, SR.C., Islamic Azad University, Tehran, Iran.

Parivash Jafari
Associate Professor, Department of Educational Administration, SR.C., Islamic Azad University, Tehran, Iran.

Abstract
The rapid advancement of information and communication technology has caused service companies, as a critical infrastructure, to face an increasing prevalence, severity, and complexity of cyber-attacks, which requires greater focus on cybersecurity. Therefore, the present study, using a multi-method qualitative approach (thematic analysis and fuzzy Delphi), has extracted, categorized, and interpreted key themes for improving cybersecurity technological capabilities. Accordingly, first, by studying and analyzing the literature on information technology capabilities and conducting semi-structured interviews with 10 managers and industrial and academic experts, and using a thematic analysis approach, technological capabilities in the field of cybersecurity were identified and categorized into 5 organizing themes and 36 basic themes. Then, the fuzzy Delphi questionnaire was distributed among 25 experts and the importance of each criterion was determined. Due to duplication or integration with other factors, 9 factors from the set of key factors of cybersecurity technological capability were screened, and ultimately, 27 basic themes or key factors were confirmed. The results showed that cybersecurity technological capability consists of 5 organizing themes, including human resource capability with 4 basic themes, organizational process capability with 3 basic themes, technical and security infrastructure capability with 9 basic themes, strategic and managerial capability with 6 basic themes, and key stakeholder security capability with 5 basic themes.

Keywords: information technology, Cyber security, technological capability, oil and gas.

[1] Corresponding Author: mrazzavi@yahoo.com