--Name of Journal---------
Vol(issue), PP.
.atu.ac.ir
DOI:

ATU PRESS

Original Research / Review / ...
Received:
Accepted:
ISSN:
eISSN:

Investigating the Impact of Information Security Knowledge Mechanism Dimensions on Protection Motivation with the Mediating Role of Psychological Processes (Case Study: National Iranian Drilling Company)

Faezeh Mayahi Arabi — Master's Degree, Department of Information Technology Management, Islamic Azad University, Ahvaz, Iran

Fariba Nazari* — Associate Professor, Department of Knowledge and Information Science, Ahvaz Branch, Islamic Azad University, Ahvaz, Iran

Abstract

The purpose of this study was to examine the impact of the dimensions of the information security knowledge mechanism on protection motivation, with psychological processes serving as a mediating factor, among employees of the National Iranian Drilling Company in Ahvaz. This research employed a descriptive-survey methodology. The statistical population consisted of all employees utilizing information systems within the company, totaling 3,200 individuals. A sample of 320 participants was selected using simple random sampling. Data were collected through a 32-item questionnaire developed by Mady et al. (2023). The proposed model was tested using SPSS version 26 and AMOS version 26. Findings indicated that knowledge breadth significantly influenced threat appraisal. Furthermore, knowledge depth and knowledge finesse

* Corresponding Author: fnazari@iau.ac.ir
How to Cite: Assistant Professor, Department of Information Science and Knowledge Studies, Ahvaz Branch, Islamic Azad University, Ahvaz, Iran

significantly affected coping appraisal. Both threat appraisal and coping appraisal had a significant impact on protection motivation.
Finally, the mediating roles of threat appraisal and coping appraisal in the relationship between knowledge breadth, depth, and finesse with protection motivation were confirmed. As a result, continuous information security training—centered on psychological processes such as threat appraisal and coping appraisal—should be implemented to align employees of the National Iranian Drilling Company with security goals. Managers and decision-makers are encouraged to enhance employees' protection motivation by developing structured programs that strengthen their information security knowledge—namely, knowledge breadth, depth, and finesse.

keywords: Information security, Protection motivation, National Iranian Drilling Company, Depth of knowledge, Psychological processes, Subtlety of knowledge, Breadth of knowledge.

--نام مجله---------
دوره ؟، شماره ؟، نام فصل، سال، ص ص
.atu.ac.ir
DOI:

مقاله پژوهشی/مروری/سخن سردبیر
تاریخ دریافت: ۰۰/۰۰/۰۰؛ تاریخ پذیرش: ۰۰/۰۰/۰۰
eISSN: ISSN:

تأثیر ابعاد ساز و کار دانش امنیت اطلاعات بر انگیزش محافظت با نقش میانجی فرآیندهای روانشناختی (مورد مطالعه: شرکت ملی حفاری ایران)

فائزه میاهی عربی کارشناسی ارشد، گروه مدیریت فناوری اطلاعات، دانشگاه آزاد اسلامی، اهواز، ایران

فریبا نظری * دانشیار، گروه علم اطلاعات و دانش شناسی، واحد اهواز، دانشگاه آزاد اسلامی، اهواز، ایران

چکیده

هدف از انجام پژوهش حاضر بررسی تأثیر ابعاد ساز و کار دانش امنیت اطلاعات بر انگیزش محافظت با نقش میانجی فرآیندهای روانشناختی در بین کارکنان شرکت ملی حفاری ایران در اهواز بود. پژوهش حاضر توصیفی- پیمایشی است. جامعه آماری کلیه کارکنان استفاده کننده از سیستم اطلاعات در شرکت ملی حفاری ایران به تعداد ۳۲۰۰ نفر است. تعداد ۳۲۰ نفر بر اساس مدلسازی معادلات ساختاری و به روش تصادفی ساده انتخاب شدند. گردآوری اطلاعات با استفاده از پرسشنامه ۳۲ سؤالی مدی و همکاران (۲۰۲۳) انجام شد. آزمون الگوی پیشنهادی، از طریق نرم‌افزارهای اس.پی.اس.اس نسخه ۲۶ و آموس نسخه ۲۶ انجام گرفت. یافته‌ها نشان داد که وسعت دانش بر نامطلوب بودن تهدید اثرگذار است. همچنین عمق دانش و ظرافت دانش بر امکان‌سنجی مقابله مؤثر بودند. نامطلوب بودن تهدید و امکان‌سنجی مقابله نیز بر انگیزش محافظت اثر معنی‌داری به جای گذاشتند. در نهایت نیز نقش میانجی نامطلوب بودن تهدید و امکان‌سنجی مقابله در تأثیر وسعت دانش، عمق دانش و ظرافت دانش بر انگیزش محافظت مورد تأیید قرار گرفت. در نتیجه برای همگام شدن کارکنان شرکت ملی حفاری ایران، باید آموزش مطلوب امنیت اطلاعات با محوریت فرایندهای روانشناختی (نامطلوب بودن تهدید و امکان‌سنجی مقابله) به صورت پیوسته ایجاد گردد و مدیران و مسئولین با برنامه‌ریزی و تقویت دانش امنیت اطلاعات (وسعت دانش، عمق دانش و ظرافت دانش) در شرکت، انگیزه انگیزش محافظت را در کارکنان بهبود بخشند.

کلیدواژه‌ها: شرکت ملی حفاری ایران، امنیت اطلاعات، انگیزش محافظت، فرآیندهای روانشناختی، ظرافت دانش، عمق دانش، وسعت دانش.

* نویسنده مسئول: fnazari@iau.ac.ir

مقدمه

در دهه‌های اخیر، تحول دیجیتال ساختار کسب‌وکارها را به‌طور بنیادین تغییر داده و وابستگی شرکت‌ها به فناوری اطلاعات افزایش یافته است. این وابستگی، در کنار مزایای فراوان، سازمان‌ها را در معرض تهدیدات سایبری پیچیده مانند بدافزارها، نفوذ به شبکه‌ها و دستکاری اطلاعات قرار داده است (شیائو[1] و همکاران، ۲۰۲۳). حوادث اخیر اهمیت حفاظت مؤثر از اطلاعات را نشان می‌دهد و پیش‌بینی می‌شود هزینه‌های جهانی خسارات سایبری تا سال ۲۰۲۵ به ۱۰٫۵ تریلیون دلار برسد (سینگ[2]، ۲۰۲۵).

امنیت اطلاعات دیگر تنها یک دغدغه فنی نیست و به مسأله‌ای رفتاری، سازمانی و راهبردی تبدیل شده است. تحقیقات نشان می‌دهند کارکنان ضعیف‌ترین حلقه در زنجیره حفاظت اطلاعات هستند و حدود ۲۵ درصد از نقض‌های اطلاعاتی ناشی از خطاهای انسانی است (مدی[3] و همکاران، ۲۰۲۳؛ منارد[4] و همکاران، ۲۰۱۷). بنابراین، شرکت‌ها به سرمایه‌گذاری در پیشگیری از چنین خطاهایی نیاز دارند. مطالعات امنیت اطلاعات، دلایل ناکافی بودن اقدامات حفاظتی کارکنان و راه‌های تشویق آن‌ها را بررسی کرده‌اند (مو[5] و همکاران، ۲۰۲۲). برای تقویت امنیت، نمی‌توان تنها به فناوری تکیه کرد و رفتار محافظتی کارکنان به‌عنوان خط مقدم دفاع سازمانی اهمیت ویژه دارد. پژوهش‌ها نشان می‌دهند انگیزش محافظت کارکنان پدیده‌ای پیچیده و چندبعدی است که تحت تأثیر عوامل مختلف قرار می‌گیرد (کرانز و هاوسینگ[6]، ۲۰۱۴؛ تران[7] و همکاران، ۲۰۲۴).

یکی از مفاهیم نوین در حوزه امنیت اطلاعات، «سازوکار دانش امنیت اطلاعات» است که برخلاف آموزش‌های صرف، بر ابعاد کیفی و شناختی دانش کارکنان تمرکز دارد. دانش امنیت اطلاعات شامل اطلاعات و مهارت‌های لازم برای محافظت از دارایی‌های اطلاعاتی سازمان مانند داده‌های مشتری، اطلاعات محصول و فروش است. فقدان این دانش ممکن است ناشی از مشارکت پایین کارکنان در تدوین سیاست‌ها یا نحوه

---

[1] Shiau et al.
[2] Singh
[3] Mady et al.
[4] Menard et al.
[5] Mou et al.
[6] Kranz & Haeussinger
[7] Tran et al.

اطلاع‌رسانی مسئولیت‌ها باشد(جانستون[1] و همکاران، ۲۰۱۹). تا زمانی که کارکنان دانش کافی نداشته باشند، سازمان‌ها در دفاع از اطلاعات خود با چالش مواجه خواهند شد (کیاشمشکی و دانشور، ۱۴۰۱). همچنین، دانش امنیتی صرفاً مبتنی بر آموزش‌های عمومی ممکن است در شرایط بحرانی کافی نباشد؛ بنابراین، توجه به ابعاد ساختاری دانش از جمله وسعت (پوشش موضوعات امنیتی)، عمق (درک مفهومی) و ظرافت (توان تحلیل موقعیت‌های خاص) ضروری است

وسعت دانش امنیت اطلاعات به میزان پوشش موضوعات امنیتی و توانایی کارکنان در استفاده از ابزارها، مهارت‌ها و منابع مرتبط اشاره دارد. عمق دانش نشان‌دهنده درک مفهومی و تخصصی فرد از مفاهیم امنیت اطلاعات است. ظرافت دانش به توانایی استفاده خلاقانه و نوآورانه از فناوری‌ها و دانش امنیتی اشاره دارد و کاربران آن قادرند راه‌حل‌های جدید ارائه دهند (تنگ و ژانگ[2]، ۲۰۲۴؛ ترابی[3] و همکاران، ۲۰۲۳). سازوکارهای دانش مانند ایجاد خط‌مشی‌ها و آموزش، انتقال دانش و مهارت‌های فنی را تسهیل می‌کنند(صفا و فون سولمز[4]، ۲۰۱۶؛ دارسی[5] و همکاران، ۲۰۱۴). با وجود تأثیر جامعیت دانش امنیتی، حوادث امنیتی همچنان رخ می‌دهند و برای تغییر رفتارهای امنیتی، صرفاً کسب دانش و آگاهی کافی نیست؛ بلکه نیاز به پر کردن شکاف بین دانش و عملکرد واقعی کارکنان وجود دارد (صفا[6] و همکاران، ۲۰۱۶؛ جانستون و همکاران، ۲۰۱۹).

ابعاد سه‌گانه دانش امنیت اطلاعات (وسعت، عمق و ظرافت دانش) نقش مهمی در شکل‌گیری نگرش، درک تهدیدها و واکنش‌های مقابله‌ای کارکنان دارند. کارمندی که درک عمیق‌تری از تهدیدات و پیامدهای رفتار خود دارد، انگیزه بیشتری برای حفاظت از خود نشان می‌دهد. این فرآیند صرفاً دانشی نیست، بلکه روان‌شناختی نیز هست و بر اساس نظریه انگیزش محافظت، افراد از طریق دو مسیر «نامطلوب بودن تهدید» و «امکان‌سنجی مقابله» به تهدیدها پاسخ می‌دهند (تانگ[7] و همکاران، ۲۰۲۱). نامطلوب نامطلوب بودن تهدید شامل حساسیت، شدت و پاداش‌های درک‌شده و امکان‌سنجی مقابله شامل

---

[1] Johnston
[2] Teng & Zhang
[3] Torabi et al.
[4] Safa & Von Solms
[5] D'Arcy et al.
[6] Safa et al.
[7] Tang et al.

خودکارآمدی، کارآیی پاسخ و هزینه‌های درک‌شده است. ترس و انگیزش محافظت نقش واسطه‌ای دارند و مسیر تبدیل دانش به رفتار پیشگیرانه را فراهم می‌کنند (خزائی‌پول و همکاران، ۱۴۰۰؛ مو و همکاران، ۲۰۲۲). بنابراین، صرف داشتن دانش یا شرکت در دوره‌های آموزشی کافی نیست؛ فرآیندهای شناختی و روان‌شناختی باید فعال شوند تا دانش به انگیزش و در نهایت رفتار حفاظتی منجر گردد. بسیاری از برنامه‌های سازمانی این جنبه‌ها را نادیده می‌گیرند و تنها بر آموزش‌های فنی تمرکز می‌کنند.

شرکت ملی حفاری ایران، به امنیت اطلاعات سطح بالا نیاز دارد. با وجود سرمایه‌گذاری‌های گسترده در زیرساخت‌ها و آموزش کارکنان، تهدیدات داخلی و نقض‌های امنیت اطلاعات همچنان گزارش می‌شوند. اگرچه پژوهش‌های متعددی به اهمیت دانش امنیت اطلاعات پرداخته‌اند، تأثیر ابعاد شناختی و ساختاری این دانش بر انگیزش محافظت، با توجه به نقش میانجی فرآیندهای روان‌شناختی، کمتر مورد بررسی تجربی قرار گرفته است. این پژوهش با هدف پر کردن این خلأ، بررسی می‌کند که آیا ابعاد دانش امنیت اطلاعات می‌توانند از مسیر درک روان‌شناختی تهدید و ارزیابی توانمندی مقابله، انگیزش محافظت واقعی کارکنان را افزایش دهند یا خیر. مسأله اصلی این است که چرا کارکنان انگیزه کافی برای رفتار ایمن ندارند و آیا مشکل از کیفیت دانش آنان است یا از درک روان‌شناختی‌شان نسبت به تهدیدات. اهمیت این موضوع در آن است که امنیت اطلاعات نه‌تنها یک الزام فناورانه، بلکه یک تعهد رفتاری و فرهنگی سازمانی است. تا زمانی که سازوکارهای شناختی و انگیزشی کارکنان فعال نشوند، احتمال بروز خطاها و نقض‌ها، حتی با بهترین ابزارهای فنی، باقی خواهد ماند.

پیشینه پژوهش

نصیری ولیک‌بنی و همکاران (۱۳۹۳) دریافتند که به‌طور کلی بین فناوری اطلاعات و امنیت روانی کارکنان رابطه معناداری وجود ندارد، هرچند برخی ابعاد فناوری اطلاعات در حوزه‌های مالی و اجرایی با کاهش امنیت روانی مرتبط بودند. میرمحمدی و همکاران (۱۳۹۵) نشان دادند که انگیزش درونی، شایستگی، معناداری و تأثیرگذاری نقش مهمی در پذیرش سیاست‌های امنیتی دارد و عوامل سازمانی مانند آموزش و مشارکت در تصمیم‌گیری‌ها بر این پذیرش تأثیرگذارند. فیروزبخت و همکاران (۱۳۹۶) تأکید کردند

که ویژگی‌های روان‌شناختی کارکنان بر درک تهدیدات و واکنش‌های مقابله‌ای آنان تأثیر دارد و انگیزه حفاظت را افزایش می‌دهد. پژوهش سبحانی‌جو و خیبری (۱۳۹۶) نشان داد که مدیریت دانش نقش تعیین‌کننده‌ای در تقویت انگیزش شغلی دارد. کریمی و پیکری (۱۳۹۷) دریافتند که آموزش و آگاهی امنیتی در میان پرستاران ادراک از شدت و قطعیت مجازات نقض سیاست‌ها را افزایش می‌دهد. همچنین عالیان و درخشنده (۱۳۹۸) تأثیر مثبت مدیریت دانش بر انگیزش کارکنان سازمان‌های خیریه و عملکرد آنان را نشان دادند. همچنین، عالی‌پور و آل‌صفری (۱۴۰۱) تأثیر رویکردهای سازمانی در حوزه آموزش امنیت، اشتراک‌گذاری دانش و مشاهده‌پذیری امنیت را بر عملکرد مدیریت امنیت اطلاعات بررسی کردند و نتایج حاکی از آن بود که این عوامل تأثیر مثبت و مستقیمی بر عملکرد امنیتی سازمان دارند و نیز نقش مهمی در ایجاد اعتماد میان کارکنان ایفا می‌کنند. عباس‌زاده و همکاران (۱۴۰۱) نیز با تحلیل روش برخورد سازمانی در اشتراک دانش، به این نتیجه رسیدند که برخورد مناسب سازمانی، مشاهده‌پذیری و اشتراک دانش می‌تواند به بهبود عملکرد امنیت اطلاعات منجر شود. همچنین، یادگیری امنیت و ثبت دانش در تقویت تعهد سازمانی نقش دارد. حسینی صیادنورد و همکاران (۱۴۰۲) نشان دادند که تعهد سازمانی، رضایت شغلی، نگرش، هنجارهای ذهنی، خودکارآمدی و هزینه پاسخ‌گویی همگی بر افزایش انگیزه حفاظت از اطلاعات تأثیر دارند و انگیزه ایجاد شده مستقیماً رفتارهای حفاظتی کارکنان را تقویت می‌کند. همچنین، ابوطالبی (۱۴۰۲) با بررسی کارکنان آتش‌نشانی دریافت که انگیزش شغلی و تسهیم دانش از طریق نقش میانجی ایمنی محیط کار با یکدیگر مرتبط‌اند و تقویت جو ایمنی و آموزش سازمانی می‌تواند به ارتقای انگیزش کارکنان کمک شایانی کند.

مطالعات پیشین نشان می‌دهند که عوامل آموزشی، شناختی و روان‌شناختی نقش مهمی در شکل‌گیری رفتارهای حفاظتی و انگیزش کارکنان در زمینه امنیت اطلاعات دارند. مرهی و میدا[1] (۲۰۱۲) دریافتند که آموزش‌ها و آگاهی‌بخشی نسبت به سیاست‌های سازمانی قصد کاربران برای تبعیت از اصول امنیت اطلاعات را افزایش می‌دهد و نگرش مثبت و درک اهمیت سیاست‌ها رفتارهای محافظتی را تقویت می‌کند. منارد و همکاران (۲۰۱۷) نشان دادند که ادراک شدت تهدید، خودکارآمدی و ارزیابی هزینه‌ها عوامل شکل‌گیری قصد رفتاری هستند و آموزش‌های هدفمند و تقویت اعتماد به نفس اهمیت

[1] Merhi & Midha

دارد. مطالعات دیگر نیز نقش عوامل سازمانی و اجتماعی را برجسته کرده‌اند. آشندن[1] (۲۰۱۸) دریافت که تفاوت دیدگاه‌ها نسبت به ریسک‌ها و رفتار همکاران، تعاملات اجتماعی و فرهنگ سازمانی بر رعایت سیاست‌های امنیتی تأثیر دارد. مو و همکاران (۲۰۲۲) با متاآنالیز بر اساس نظریه انگیزش محافظت نشان دادند که امکان‌سنجی مقابله مهم‌ترین عامل در رفتار حفاظتی است. گو[2] و همکاران (۲۰۲۲) تأثیر پیام‌های آموزشی ساختاریافته بر ادراک تهدید و رفتار محافظتی را بررسی کردند و مدی و همکاران (۲۰۲۳) نقش سازوکارهای دانش سازمانی در افزایش انگیزش حفاظتی کارکنان را تأیید نمودند.

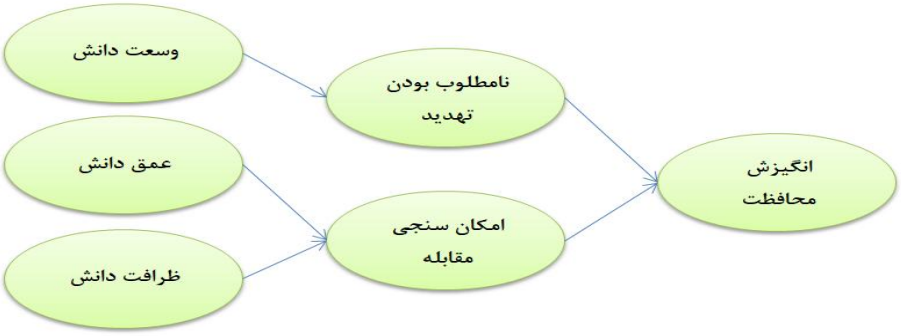
تحقیقات اخیر نیز بر اهمیت فرآیندهای روان‌شناختی و نقش دانش در شکل‌دهی رفتارهای محافظتی تأکید دارند. تران و همکاران (۲۰۲۴) نشان دادند که آگاهی از امنیت سایبری انگیزش و رفتار محافظتی را افزایش می‌دهد، گابالدون[3] و همکاران (۲۰۲۴) خطاهای شناختی را به‌عنوان واسطه بین آسیب‌پذیری و هزینه پاسخ شناسایی کردند و چائه[4] (۲۰۲۵) اثر واسطه‌ای مقابله در ارتباط بین تهدید درک‌شده و رفاه روانی را بررسی کرد. الشمری و الممارى[5] (۲۰۲۵) مدلی یکپارچه ارائه دادند که عوامل شناختی، انگیزشی و رفتاری را در رعایت سیاست‌های امنیتی ترکیب می‌کند و عبداللطیف[6] و همکاران (۲۰۲۵) نشان دادند که پاسخ‌های عاطفی نقش واسطه‌ای در انگیزه محافظت دارند.

مرور پیشینه داخلی و خارجی نشان می‌دهد که بیشتر پژوهش‌ها به‌صورت جداگانه به موضوعاتی مانند مدیریت دانش، امنیت اطلاعات، انگیزش شغلی یا متغیرهای روان‌شناختی پرداخته‌اند و در اغلب آنها، ارتباط میان دانش امنیت اطلاعات و رفتارهای محافظتی به‌طور مستقیم و بدون توجه به سازوکارهای روان‌شناختی تحلیل شده است. نوآوری اصلی تحقیق حاضر در تلفیق سه حوزه مفهومی کلیدی شامل «ابعاد سازوکار دانش امنیت اطلاعات»، «انگیزش محافظت» و «فرآیندهای روان‌شناختی» در قالب یک مدل علّی و ساختاری است. به‌ویژه، استفاده از فرآیندهای روان‌شناختی به‌عنوان متغیر میانجی میان سازوکارهای دانشی و انگیزش محافظتی، وجه تمایز مهم این پژوهش نسبت به تحقیقات پیشین محسوب می‌شود. علاوه بر این، در پژوهش‌های پیشین مدیریت دانش معمولاً به‌طور کلی بررسی شده

---

[1] Ashenden
[2] Goh
[3] Gabaldon et al.
[4] Chae
[5] Alshammari & Al-Mamary
[6] Abd Latif et al.

است، در حالی‌که تحقیق حاضر با تمرکز بر ابعاد مشخص سازوکارهای دانش امنیت اطلاعات شامل ثبت، تسهیم، به‌کارگیری و یادگیری امنیتی، دیدگاهی دقیق‌تر و عمیق‌تر ارائه می‌دهد. اجرای پژوهش در سازمانی تخصصی و راهبردی مانند شرکت ملی حفاری ایران نیز بُعد کاربردی ویژه‌ای به تحقیق بخشیده و زمینه تعمیم و بهره‌برداری از نتایج را فراهم می‌سازد. به طور کلی، تحقیق حاضر از نظر ساختار مفهومی، نحوه ترکیب متغیرها، دیدگاه روان‌شناختی و زمینه کاربردی، نوآوری قابل توجهی نسبت به مطالعات پیشین دارد. پیشینه‌ها، با ارائه اطلاعات موضوعی، مقیاس‌های اندازه‌گیری و دیدگاه‌های متنوع نسبت به انگیزش محافظت، بستر مناسبی برای اجرای بهتر پژوهش فراهم کرده‌اند. با وجود آنکه مطالعه مشابه داخلی و خارجی دقیقاً با عنوان حاضر مشاهده نشد، بررسی تأثیر ابعاد سازوکار دانش امنیت اطلاعات بر انگیزش محافظت با نقش میانجی فرآیندهای روان‌شناختی همچنان نیازمند مطالعات بیشتر است. مدل مفهومی تحقیق به صورت است:



شکل ۱: مدل پژوهش (مدی و همکاران، ۲۰۲۳)

فرضیه‌های پژوهش به صورت زیر است:

فرضیه‌های اصلی:

فرضیه اصلی اول) وسعت دانش امنیت اطلاعات بر انگیزش محافظت با نقش میانجی نامطلوب بودن تهدید در شرکت ملی حفاری ایران تأثیر مثبت و غیرمستقیمی دارد.

فرضیه اصلی دوم) عمق دانش امنیت اطلاعات بر انگیزش محافظت با نقش میانجی امکان‌سنجی مقابله در شرکت ملی حفاری ایران تأثیر مثبت و غیرمستقیمی دارد.

فرضیه اصلی سوم) ظرافت دانش امنیت اطلاعات بر انگیزش محافظت با نقش میانجی امکان‌سنجی مقابله در شرکت ملی حفاری ایران تأثیر مثبت و غیرمستقیمی دارد.

فرضیه‌های فرعی:

فرضیه فرعی اول) وسعت دانش امنیت اطلاعات بر نامطلوب بودن تهدید در میان کارکنان شرکت ملی حفاری ایران تأثیر مثبت و مستقیمی دارد.

فرضیه فرعی دوم) عمق دانش امنیت اطلاعات بر امکان‌سنجی مقابله در میان کارکنان شرکت ملی حفاری ایران تأثیر مثبت و مستقیمی دارد.

فرضیه فرعی سوم) ظرافت دانش امنیت اطلاعات بر امکان‌سنجی مقابله در میان کارکنان شرکت ملی حفاری ایران تأثیر مثبت و مستقیمی دارد.

فرضیه فرعی چهارم) نامطلوب بودن تهدید بر انگیزش محافظت در میان کارکنان شرکت ملی حفاری ایران تأثیر مثبت و مستقیمی دارد.

فرضیه فرعی پنجم) امکان‌سنجی مقابله بر انگیزش محافظت در میان کارکنان شرکت ملی حفاری ایران تأثیر مثبت و مستقیمی دارد.

روش

مطالعه حاضر از نظر هدف کاربردی، از نظر ماهیت علّی و از نظر روش توصیفی-پیمایشی است. جامعه آماری این پژوهش شامل تمامی کارکنان شرکت ملی حفاری ایران است که در انجام وظایف شغلی خود با سیستم‌های اطلاعاتی سازمان کار می‌کنند. تعداد این افراد طبق آمار ارائه‌شده توسط اداره منابع انسانی شرکت در سال ۱۴۰۳، برابر با ۳۲۰۰ نفر می‌باشد.

برای تعیین حجم نمونه، از قاعده پیشنهادی در مدلسازی معادلات ساختاری استفاده شد که بر مبنای آن، حجم نمونه بین ۵ تا ۱۵ مشاهده به ازای هر سازه پرسشنامه پیشنهاد می‌شود (هومن، ۱۳۹۷؛ کلانتری، ۱۳۹۴). با توجه به ۳۲ گویه، دامنه حجم نمونه بین ۱۶۰ تا ۴۸۰ نفر است. بر این اساس، با رویکرد محافظه‌کارانه، حجم نمونه ۳۲۰ نفر انتخاب شد. روش نمونه‌گیری تصادفی ساده است. از میان ۴۰۰ پرسشنامه توزیع‌شده، ۳۴۱ پرسشنامه عودت داده شد و پس از بررسی ۲۱ پرسشنامه مخدوش، تعداد ۳۲۰ مورد معتبر تحلیل شد (نرخ بازگشت: ۸۵٪).

برای جمع‌آوری اطلاعات، از پرسشنامه‌ای استفاده شده که شامل دو بخش سوالات جمعیت‌شناختی و سوالات تخصصی می‌باشد. بخش جمعیت‌شناختی شامل اطلاعاتی مانند

جنسیت، سن، سطح تحصیلات و سابقه کاری است. در حالی که سوالات تخصصی برگرفته از پرسشنامه‌ای با ۳۲ سؤال طراحی شده توسط مدی و همکاران (۲۰۲۳) هستند که شامل مواردی چون وسعت دانش امنیت اطلاعات (سؤالات ۱ الی ۳)، عمق دانش امنیت اطلاعات (سؤالات ۴ الی ۶)، ظرافت دانش امنیت اطلاعات (سؤالات ۷ الی ۹)، نامطلوب بودن تهدید (سؤالات ۱۵ الی ۲۶) و امکان‌سنجی مقابله (سؤالات ۲۷ الی ۳۲) می‌باشد. در این پرسشنامه از مقیاس پنج گزینه‌ای لیکرت برای پاسخ‌دهی استفاده شده که دامنه پاسخ‌ها از «کاملاً موافقم» تا «کاملاً مخالفم» تنظیم شده است. برای ارزیابی روایی و پایایی پرسشنامه، دو نوع روایی یعنی روایی صوری[1] و روایی سازه[2] مورد بررسی قرار گرفتند. اعتبار صوری پرسشنامه با تأیید کارشناسان و استادان حوزه مدیریت تأمین شد و از این منظر دارای اعتبار لازم بود. همچنین روایی سازه با استفاده از روش روایی همگرا[3] و با بهره‌گیری از شاخص میانگین واریانس استخراجی[4] فورنل و لارکر[5] (۱۹۸۱) مورد بررسی قرار گرفت. برای سنجش پایایی نیز، یک نمونه اولیه شامل ۳۰ پرسشنامه پیش‌آزمون شد و سپس با استفاده از داده‌های جمع‌آوری شده، پایایی به روش آلفای کرونباخ محاسبه گردید که نتایج آن در جدول ۱ ارائه شده است.

جدول ۱. روایی و پایایی متغیرها

نام متغیر	آلفای کرونباخ	پایایی مرکب	میانگین واریانس استخراجی	CR>AVE
وسعت دانش	۰/۸۴۱	۰/۸۶۱	۰/۶۷۵	تأیید
عمق دانش	۰/۷۵۲	۰/۸۱۳	۰/۵۹۴	تأیید
ظرافت دانش	۰/۸۱۲	۰/۸۲۹	۰/۶۲۱	تأیید
انگیزش محافظت	۰/۸۲۵	۰/۸۴۰	۰/۵۱۳	تأیید
نامطلوب بودن تهدید	۰/۹۱۶	۰/۹۲۶	۰/۷۵۹	تأیید
امکان‌سنجی مقابله	۰/۸۸۱	۰/۸۸۷	۰/۷۹۸	تأیید

[1] Content Validity
[2] Construct Validity
[3] Convergent Validity
[4] Average Variances Extracted (AVE)
[5] Fornell & Larcker

جدول فوق مقادیر روایی را برای تمامی متغیرها نشان می‌دهد که مقادیر بالای ۰/۵ به عنوان مقادیر مطلوب شناخته می‌شوند. نتایج نشان‌دهنده وجود روایی همگرا بین شاخص های سازه اصلی پژوهش است. برای ارزیابی پایایی پرسشنامه، از پایایی مرکب و آلفای کرونباخ استفاده شد. همچنین پایایی مرکب هر یک از متغیرها دارای مقادیری بالاتر از ۰/۷ بود که نشان‌دهنده همبستگی بالا میان متغیرها است. همچنین بر اساس نتایج، پرسشنامه از پایایی کافی برخوردار است.

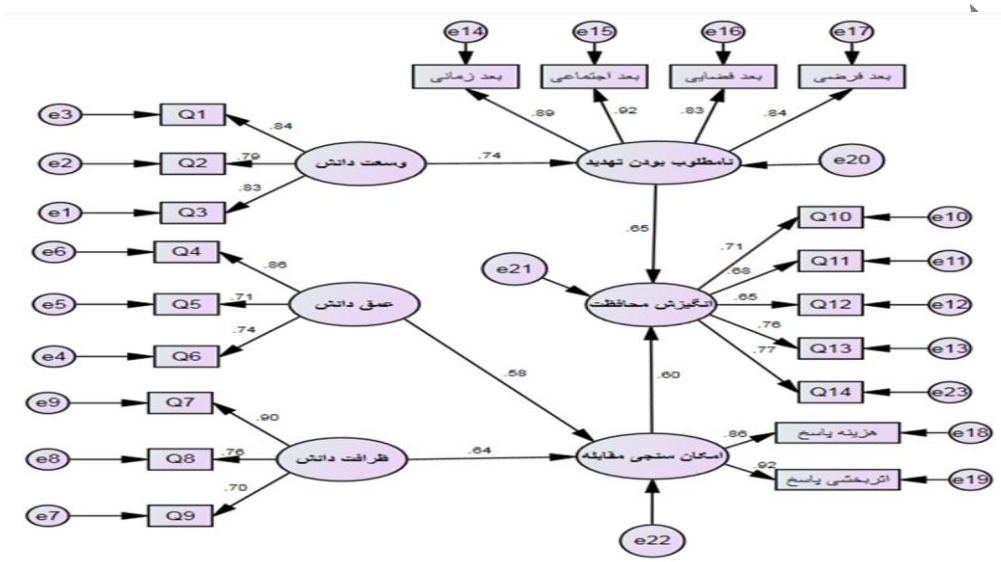
یافته‌ها

طبق داده‌های موجود در جدول (۲)، در میان پاسخ‌دهندگان ۷۰/۳ درصد مرد و ۲۹/۷ درصد زن هستند که نشان‌دهنده سهم بیشتر مردان در نمونه است. در خصوص سن، ۵/۳ درصد از کارکنان زیر ۳۰ سال، ۳۲/۵ درصد بین ۳۱ تا ۴۰ سال، ۳۴/۷ درصد بین ۴۱ تا ۵۰ سال و ۲۷/۵ درصد بالای ۵۰ سال هستند. همچنین، در زمینه تحصیلات، ۴/۸ درصد دارای دیپلم و پایین‌تر، ۱۴/۱ درصد کاردانی، ۴۳/۴ درصد کارشناسی، ۳۲/۲ درصد کارشناسی ارشد و ۱/۹ درصد دکتری می‌باشند.

جدول ۲: مشخصات جمعیت‌شناختی

سن	فراوانی	سابقه کار	فراوانی
زیر ۳۰ سال	۱۷	زیر۵ سال	۲۱
۳۱ تا ۴۰ سال	۱۰۴	۵ تا ۱۰ سال	۸۶
۴۱ تا ۵۰ سال	۱۱۱	۱۱ تا ۱۵ سال	۹۵
بالای ۵۰ سال	۸۸	بالای ۱۵ سال	۱۱۸
میزان تحصیلات	**فراوانی**	**جنسیت**	**فراوانی**
دیپلم و پایین‌تر	۲۷	زن	۹۵
کاردانی	۴۵	مرد	۲۲۵
کارشناسی	۱۳۹		
کارشناسی ارشد	۱۰۳		
دکتری	۶		

برای آزمون فرضیه‌ها پژوهش، از مدلسازی معادلات ساختاری با استفاده از نرم‌افزار آموس بهره گرفته شد. مدل پژوهش به همراه ضرایب استاندارد در شکل ۲ نمایش داده شده و نتایج آن در جدول ۴ ارائه گردیده است.



شکل ۲: مدل پژوهش با ضرایب استاندارد شده بار عاملی (ارزیابی مدل‌های اندازه‌گیری)

پیش از بررسی فرضیه‌ها شاخص‌های برازش باید بررسی شوند:

جدول ۳. شاخص‌های برازش

شاخص	شاخص			مقدار محاسبه شده
	علامت اختصاصی	معادل فارسی	دامنه قابل قبول	در پژوهش حاضر
تطبیقی (نسبی)	NFI	شاخص نرم‌شده برازندگی	>۰/۸۰	۰/۹۴۸
	CFI	شاخص برازش تطبیقی	۰/۹۰ و بیشتر	۰/۹۵۲
	RFI	شاخص برازندگی فزاینده	۰/۹۰ و بیشتر	۰/۹۲۷
	χ^2/df	مجذور کای نسبی	کمتر از ۳	۱/۹۷۷
مقتصد	RMSEA	ریشه میانگین مربعات تقریب	۰/۰۸-۰	۰/۰۵۹
مطلق	GFI	شاخص نیکویی برازش	نزدیک ۱	۰/۹۲۲
	AGFI	شاخص نیکویی برازش اصلاح‌شده	نزدیک ۱	۰/۸۸۲
	Chi-Square	کای دو	وابسته به حجم نمونه	۱۳۸/۴۱۵

همان‌طور که در جدول ۳ مشاهده می‌شود، با توجه به معیارهای برازندگی، به ویژه نسبت مجذور کای به درجه آزادی که برابر با ۱/۹۷۷ است (ملاک کمتر از ۳)، شاخص نیکویی برازش (GFI) برابر با ۰/۹۲۲، شاخص نیکویی برازش تعدیل‌یافته (AGFI) برابر با ۰/۸۸۲، شاخص برازندگی مقایسه‌ای (RFI) برابر با ۰/۹۲۷، شاخص برازندگی افزایشی (CFI) برابر با ۰/۹۵۲ و ریشه خطای تقریب میانگین مجذورات (RMSEA) برابر با ۰/۰۵۹ می‌باشد. این نتایج نشان‌دهنده برازندگی مناسب مدل نهایی است. همچنین، تمامی روابط بین متغیرها در مدل در سطح معناداری P<۰/۰۵ قابل توجه هستند.

جدول ۴: نتایج فرضیه‌های فرعی پژوهش

مسیر مستقیم	ضریب تأثیر (β)	عدد معناداری (t-value)	سطح معنی‌داری	نتیجه
وسعت دانش امنیت اطلاعات ← نامطلوب بودن تهدید	۰/۷۴	۱۲/۹۶۷	۰/۰۰۰	تأیید فرضیه
عمق دانش← امکان‌سنجی مقابله	۰/۵۸	۱۰/۵۵۱	۰/۰۰۰	تأیید فرضیه
ظرافت دانش امنیت اطلاعات ← امکان‌سنجی مقابله	۰/۶۴	۱۰/۷۷۵	۰/۰۰۰	تأیید فرضیه
نامطلوب بودن تهدید ← انگیزش محافظت	۰/۶۵	۱۱/۹۱۵	۰/۰۰۰	تأیید فرضیه
امکان‌سنجی مقابله ← انگیزش محافظت	۰/۶۰	۱۱/۱۲۸	۰/۰۰۰	تأیید فرضیه

همان‌طور که در جدول ۴ مشخص است، مقدار مطلق آماره t برای تمامی فرضیه‌ها پژوهش بالاتر از مقدار مطلق ۱/۹۶ است. بنابراین می‌توان نتیجه گرفت که تمامی فرضیه‌ها فرعی تأیید شده‌اند. نتایج تحلیل بوت استرپینگ که در جدول (۵) آمده است.

جدول ۵: نتایج فرضیه‌ها میانجی‌گر

مسیر	اثر کامل		اثر غیر مستقیم (نقش میانجی)		نتیجه
	ضریب تأثیر (β)	سطح معناداری	ضریب تأثیر (β)	سطح معناداری	
نقش میانجی نامطلوب بودن تهدید در تأثیر وسعت دانش امنیت اطلاعات بر انگیزش محافظت	۰/۴۸۷	p<۰/۰۵	۰/۴۸۷	p<۰/۰۵	تأیید
نقش میانجی امکان سنجی مقابله در تأثیر عمق دانش امنیت اطلاعات بر انگیزش محافظت	۰/۳۵۲	p<۰/۰۵	۰/۳۵۲	p<۰/۰۵	تأیید
نقش میانجی امکان سنجی مقابله در تأثیر ظرافت دانش امنیت اطلاعات بر انگیزش محافظت	۰/۳۸۷	p<۰/۰۵	۰/۳۸۷	p<۰/۰۵	تأیید

نشان جدول ۵ می‌دهد که مقدار سطح معناداری آزمون برای فرضیه‌ها اصلی کمتر از ۰/۰۵ است؛ بنابراین فرضیه‌های اصلی نیز تأیید می‌شوند.

بحث و نتیجه‌گیری

شرکت‌های فعال در یک صنعت معمولاً در محیط‌های مشابه فعالیت می‌کنند و از فرآیندهای فناوری اطلاعات مشترک استفاده می‌نمایند، بنابراین آسیب‌پذیری‌های امنیت اطلاعات در یک شرکت می‌تواند بازتاب مشکلات رایج میان همتایان باشد. یکی از راهکارهای مقابله با این مشکلات، برگزاری دوره‌های آموزشی برای کارکنان است که دانش آنان را ارتقا می‌دهد. شواهد نظری و تجربی نشان می‌دهد که ابعاد سازوکار دانش امنیت اطلاعات بر انگیزش محافظت، بر فرآیندهای روان‌شناختی و به‌طور غیرمستقیم از طریق فرآیندهای روان‌شناختی بر انگیزش محافظت تأثیرگذارند. با این حال، این روابط تاکنون در کارکنان شرکت ملی حفاری ایران بررسی نشده است. بر این اساس، پژوهش حاضر با هدف بررسی تأثیر ابعاد سازوکار دانش امنیت اطلاعات (وسعت، عمق و ظرافت دانش) بر انگیزش محافظت و نقش میانجی فرآیندهای روان‌شناختی (نامطلوب بودن تهدید و امکان‌سنجی مقابله) با استفاده از مدلسازی معادلات ساختاری انجام شده است.

نتایج پژوهش نشان می‌دهد که وسعت دانش امنیت اطلاعات تأثیر مثبت و مستقیم بر نامطلوب بودن تهدید دارد؛ به این معنا که دانش گسترده کارکنان نسبت به امنیت اطلاعات، درک آن‌ها از شدت و مخاطرات تهدیدات را افزایش می‌دهد. این یافته با نتایج نصیری ولیک‌بنی و همکاران (۱۳۹۳) همخوانی دارد که نشان داده‌اند دانش فناوری اطلاعات هرچند ممکن است تأثیر مستقیم بر امنیت روانی نداشته باشد، اما ادراک تهدیدات را تقویت می‌کند. همچنین کریمی و پیکری (۱۳۹۷) نیز تأکید کرده‌اند که آموزش و آگاهی امنیتی می‌تواند درک کارکنان از شدت تهدیدات را افزایش دهد، که اهمیت گسترش دانش امنیتی در شکل‌گیری نگرش‌های محافظتی را تأیید می‌کند.

در مورد عمق دانش امنیت اطلاعات، نتایج فرضیه دوم فرعی نشان داد که دانش تخصصی و کیفی، امکان‌سنجی مقابله کارکنان را تقویت می‌کند؛ یعنی آنان باور بیشتری به توانایی مدیریت و مقابله با تهدیدات دارند. این یافته با نتایج فیروزبخت و همکاران (۱۳۹۶) مطابقت دارد که بر نقش خودکارآمدی و باور به اثربخشی اقدامات مقابله‌ای در

انگیزه‌های حفاظتی تأکید کرده‌اند. همچنین، حسینی صیادنورد و همکاران (۱۴۰۲) نشان دادند که باور به امکان مقابله یکی از عوامل اساسی افزایش انگیزش حفاظت است. بنابراین، عمق دانش امنیتی به‌عنوان زیرساخت اعتماد به توان مقابله، نقش حیاتی در تقویت اقدامات پیشگیرانه ایفا می‌کند.

در تأیید فرضیه سوم فرعی، نتایج پژوهش نشان می‌دهد که ظرافت دانش امنیت اطلاعات به‌طور مستقیم بر امکان‌سنجی مقابله تأثیر مثبت دارد؛ یعنی دانش دقیق و تخصصی توانمندی کارکنان در درک پیچیدگی تهدیدات و انتخاب راهکارهای مقابله‌ای مناسب را افزایش می‌دهد. این یافته با نتایج عالی‌پور و آل‌صفری (۱۴۰۱) همسو است که نقش دانش ظریف و تخصصی را در بهبود عملکرد امنیتی و افزایش اعتماد به سازمان برجسته کرده‌اند. چنین دانش ظریف به کارکنان امکان می‌دهد نه تنها تهدیدات را بهتر شناسایی کنند، بلکه راهکارهای مقابله‌ای مؤثرتر و متناسب با شرایط اتخاذ نمایند.

فرضیه چهارم فرعی مبنی بر تأثیر مثبت و مستقیم نامطلوب بودن تهدید بر انگیزش محافظت نیز تأیید شد که نشان می‌دهد درک تهدیدات به عنوان خطرات واقعی و نامطلوب، محرک قوی برای افزایش انگیزه کارکنان جهت انجام اقدامات حفاظتی است. این نتایج با پژوهش‌های مدی و همکاران (۲۰۲۳) و منارد و همکاران (۲۰۱۷) تطابق دارد که شدت تهدید را به عنوان عامل اصلی فعال‌کننده رفتارهای حفاظتی معرفی کرده‌اند. به عبارت دیگر، احساس خطر و شناخت عمق تهدید، کارکنان را وادار می‌سازد تا در راستای کاهش ریسک، فعالانه‌تر عمل کنند.

همچنین، تأیید فرضیه پنجم فرعی مبنی بر تأثیر مثبت و مستقیم امکان‌سنجی مقابله بر انگیزش محافظت بیانگر این است که باور به توانایی مقابله و اثربخشی راهکارهای دفاعی، عاملی تعیین‌کننده در ارتقاء انگیزش حفاظت است. این موضوع به خوبی با یافته‌های مو و همکاران (۲۰۲۲) همسویی دارد که خودکارآمدی و باور به اثربخشی اقدامات مقابله‌ای را محرک اصلی رفتارهای امنیتی معرفی کرده‌اند. باور به امکان مقابله، باعث می‌شود که کارکنان بیشتر به انجام اقدامات حفاظتی تمایل داشته باشند و از بی‌تفاوتی نسبت به تهدیدات جلوگیری شود.

فرضیه‌های اصلی پژوهش نیز که نقش میانجی نامطلوب بودن تهدید و امکان‌سنجی مقابله را در روابط بین ابعاد مختلف دانش امنیت اطلاعات و انگیزش محافظت بررسی

کردند، به طور کامل تأیید شدند. تأیید فرضیه اول اصلی نشان می‌دهد که وسعت دانش امنیت اطلاعات از طریق افزایش ادراک نامطلوب بودن تهدید، انگیزش محافظت را به شکل غیرمستقیم و مثبتی تقویت می‌کند. این یافته با پژوهش آشندن (۲۰۱۸) و گوه و همکاران (۲۰۲۲) که به اهمیت ادراک تهدید به عنوان واسطه بین دانش و رفتارهای حفاظتی اشاره کرده‌اند، هم‌راستا است. به عبارت دیگر، دانش وسیع بدون درک جدی از تهدیدات نمی‌تواند به شکل موثری انگیزش حفاظت را افزایش دهد.

در فرضیه دوم اصلی، عمق دانش امنیت اطلاعات با واسطه امکان‌سنجی مقابله، تأثیر مثبت و غیرمستقیمی بر انگیزش محافظت دارد. این موضوع نشان می‌دهد که دانش عمیق به خودی خود کافی نیست؛ بلکه باید این دانش منجر به باور به توانایی مقابله و اثربخشی اقدامات شود تا انگیزش حفاظتی به طور موثری افزایش یابد. این موضوع در مطالعات مو و همکاران (۲۰۲۲) و منارد و همکاران (۲۰۱۷) نیز به روشنی بیان شده است، که بر نقش کلیدی خودکارآمدی در فرآیند محافظتی تأکید دارند.

فرضیه سوم اصلی نیز که تأثیر غیرمستقیم ظرافت دانش امنیت اطلاعات بر انگیزش محافظت از طریق امکان‌سنجی مقابله را بررسی کرد، تایید شده است. این نشان می‌دهد که دانش تخصصی و دقیق، با ارتقاء باور به توان مقابله، به شکل موثری انگیزش حفاظت را تقویت می‌کند. یافته‌های عالی‌پور و آل-صفری (۱۴۰۱) و عباس‌زاده و همکاران (۱۴۰۱) که ظرافت دانش را به عنوان کلید موفقیت در افزایش تعهد و عملکرد امنیتی معرفی کرده‌اند، این نتیجه را تأیید می‌کنند. بنابراین، توسعه دانش ظریف امنیتی باید در سیاست‌های آموزشی سازمان‌ها مورد توجه ویژه قرار گیرد تا انگیزش حفاظتی در کارکنان به حداکثر برسد.

نتایج پژوهش نشان می‌دهد که دانش امنیت اطلاعات در سه بُعد وسعت، عمق و ظرافت، از طریق درک تهدیدات و باور به توان مقابله، انگیزش حفاظت کارکنان را به طور معناداری افزایش می‌دهد. این یافته‌ها تأکید می‌کنند که صرف داشتن دانش کافی کافی نیست و برای ایجاد انگیزش موثر، درک عمیق از تهدیدات و اعتماد به راهکارهای مقابله‌ای ضروری است. بنابراین، ارتقاء ابعاد مختلف دانش امنیت اطلاعات از طریق آموزش‌های هدفمند و تقویت فرآیندهای روانشناختی، به ویژه در میان کارکنان شرکت ملی حفاری ایران، می‌تواند انگیزش محافظت و در نتیجه امنیت اطلاعات را بهبود بخشد.

بر اساس نتایج، پیشنهاد می‌شود برنامه‌های آموزشی منظم و کاربردی در حوزه امنیت اطلاعات طراحی و اجرا شود تا دانش کارکنان تقویت و انگیزش محافظت افزایش یابد.بر اساس نتایج به دست آمده، پیشنهادات زیر ارائه می‌شود.

-شرکت باید به طور مستمر و جامع برنامه‌های آموزشی در زمینه امنیت اطلاعات را برای تمام کارکنان اجرا کند. این آموزش‌ها باید شامل مباحثی نظیر تعریف و انواع تهدیدات امنیتی، روش‌های کاهش این تهدیدات، بهترین شیوه‌های حفاظت از داده‌ها و سیاست‌های امنیتی سازمان باشد. همچنین، ارزیابی پیوسته سطح دانش و آگاهی کارکنان در این حوزه ضروری است.

-برگزاری کارگاه‌ها و سمینارهای تخصصی در زمینه امنیت اطلاعات باید به عنوان فرصتی برای کارکنان فراهم شود تا بتوانند دانش خود را در زمینه‌های مختلف امنیتی مانند مدیریت ریسک، مهندسی امنیت، دفاع سایبری و تحلیل تهدیدات افزایش دهند. همچنین، دسترسی به منابع آموزشی به‌روز در این حوزه باید برای کارکنان فراهم گردد.

-شرکت باید با بهره‌گیری از تجربیات و دانش کارشناسان امنیت اطلاعات، راهکارهای فنی مؤثری را برای کاهش تهدیدات شناسایی کرده و در اختیار کارکنان قرار دهد. این راهکارها ممکن است شامل استفاده از ابزارهای امنیتی پیشرفته، اجرای پروتکل‌های امنیتی مناسب و به کارگیری فناوری‌های نوین برای حفاظت از اطلاعات باشد. همچنین، آموزش عملی در مورد این راهکارها برای کارکنان الزامی است.

-ایجاد یک سیستم هشدار سریع به منظور شناسایی و پاسخ به تهدیدات امنیتی در حال وقوع ضروری است.

-برای حفاظت از اطلاعات و سیستم‌های اطلاعاتی شرکت در برابر تهدیدات امنیتی، باید یک سیستم مدیریت امنیت اطلاعات پیاده‌سازی شود. این سیستم فرآیندهای منسجم و ساختاریافته‌ای را برای شناسایی، ارزیابی و مدیریت ریسک‌های امنیتی ارائه می‌دهد. همچنین، برگزاری آموزش‌های هدفمند برای کارکنان ضروری است تا آنها با چالش‌های امنیتی آشنا شوند.

-طراحی و پیاده‌سازی سیستم‌های پاداش و انگیزشی برای کارکنان فعال در زمینه امنیت اطلاعات می‌تواند به تقویت انگیزه آنها در حفظ دارایی‌های اطلاعاتی کمک کند.

محدودیت‌های پژوهش عبارتند از:

موانع و محدودیت‌های پژوهش عبات بودند از:

- محدودیت دسترسی به اطلاعات: به دلیل حساسیت موضوع امنیت اطلاعات، پژوهشگر با محدودیت در دسترسی به اطلاعات و داده‌های مورد نیاز برای پژوهش روبرو شد.
- محدودیت زمانی و هزینه‌ای: جمع‌آوری و تحلیل داده‌های مربوط به چندین بعد دانش امنیت اطلاعات و فرایندهای روانشناختی، نیازمند زمان و هزینه بیشتری بود.
- محدودیت عمومی‌سازی نتایج: با توجه به ویژگی‌های خاص شرکت ملی حفاری ایران، امکان تعمیم نتایج پژوهش به سایر شرکت‌ها و صنایع محدود است.
- محدودیت در درک پیچیدگی روابط میان متغیرها: تعیین و آزمون روابط میان ابعاد دانش امنیت اطلاعات، فرایندهای روانشناختی و انگیزش محافظت چالش برانگیز بود، زیرا این متغیرها ممکن است دارای تعامل‌های چندگانه و غیرخطی باشند.
- محدودیت در یکپارچه‌سازی دانش میان رشته‌ای: این پژوهش نیازمند یکپارچه‌سازی دانش میان حوزه‌های امنیت اطلاعات، روانشناسی و رفتار سازمانی بود که دشوار و زمان‌بر بود.

تعارض منافع

نویسندگان هیچ گونه تعارض منافعی ندارند.

سپاسگزاری

از کلیه کارکنان سیستم اطلاعات در شرکت ملی حفاری ایران تقدیر و تشکر به عمل می‌آید.

ORCID

Faeze Mayahi Arabi http://orcid.org/0000-0003-2388-3507

Fariba Nazari http://orcid.org/0009-0005-2886-4200

منابع

ابوطالبی، علیرضا. (۱۴۰۲). بررسی رابطه انگیزش شغلی و تسهیم دانش با نقش میانجی ایمنی در محیط کار در پرسنل آتش نشانی قم. *هشتمین کنفرانس ملی رویکردهای نوین در آموزش و پژوهش، محمودآباد.*

حسینی صیادنورد، منیره؛ جهدی، علی؛ کیاکجوری، کریم. (۱۴۰۲). تأثیر عوامل سازمانی مرتبط با کار، انگیزه حفاظت و رفتار برنامه ریزی شده بر حفاظت از امنیت اطلاعات در سازمان کشتیرانی جمهوری اسلامی ایران. *فصلنامه آموزش علوم دریایی، ۱۰*(۳)، ۹۵-۱۰۸.

خزائی پول، مریم؛ نقیبی، ابوالحسن؛ پاشائی، طاهره؛ چالشگر کردآسیابی، مشرفه. (۱۴۰۰). کاربرد تئوری انگیزش محافظت در ارزیابی رفتارهای پیشگیری کننده از کووید-۱۹. مجله دانشگاه علوم پزشکی مازندران، ۳۱(۱۹۵)، ۲۰-۲۹.

سبحانی جو، باقر؛ خیبری، محمد. (۱۳۹۶). بررسی رابطه بین مدیریت دانش با انگیزش شغلی در کارکنان اداره کل ورزش و جوانان استان اهواز. *اولین همایش ملی دستاوردهای علوم ورزشی و سلامت دانشگاه علوم پزشکی آبادان، اهواز.*

عالیان، رشدیه؛ درخشنده، رضا. (۱۳۹۸). بررسی تأثیر مدیریت دانش بر انگیزش کارکنان اوقاف و امور خیریه استان هرمزگان. *کنفرانس ملی پژوهش های حرفه‌ای در روانشناسی و مشاوره با رویکرد دستاورهای نوین در علوم تربیتی و رفتاری «از نگاه معلم»، میناب.*

عالی‌پور، نعمت‌اله؛ آل‌صفری، نظام. (۱۴۰۱). بررسی و تحلیل تأثیر رویکردهای سازمانی آموزش امنیت اشتراک گذاری دانش، تحصیلات امنیتی و مشاهده‌پذیری امنیت بر عملکرد مدیریت امنیت اطلاعات. *سومین کنفرانس بین‌المللی چالش‌ها و راهکارهای نوین در مهندسی صنایع، مدیریت و حسابداری، چابهار.*

عباس‌زاده، ادریس؛ ثنایی، محمدرضا؛ احتشام راثی، رضا. (۱۴۰۱). تأثیر روش برخورد سازمانی در اشتراک دانش بر کارکرد مدیریت امنیت اطلاعات. *سامانه‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند، ۳*(۱)، ۲۵-۳۵.

فیروزبخت، مهرشید؛ عیدی، فاطمه؛ یوسفی‌پور، محمد. (۱۳۹۶). بررسی رابطه روانشناسی کارمندان داخلی سازمان با تهدید امنیت اطلاعات و ارزیابی مقابله با تهدید. *نخستین کنفرانس ملی پیشرفت‌ها و فرصت‌های فناوری اطلاعات و ارتباطات، تهران.*

کریمی، زهرا؛ پیکری، حمید رضا. (۱۳۹۷). تأثیر ادراک پرستاران از آموزش امنیت اطلاعات و آگاهی از سیاست‌های امنیت اطلاعات بر ادراک از شدت و قطعیت مجازات نقض امنیت اطلاعات (مورد مطالعه بیمارستان‌های تخصصی آموزشی شهر اصفهان). *آموزش پرستاری، ۷*(۲)، ۱۷-۲۴.

کلانتری، خلیل. (۱۳۹۴). مدل‌سازی معادلات ساختاری در پژوهش‌های اجتماعی و اقتصادی (با نرم‌افزارهای لیسرل و سیمپلیس). *تهران: انتشارات آگاه.*

کیاشمشکی، محمدعلی؛ دانشور، امیر. (۱۴۰۱). به کار گیری مدلسازی معادلات ساختاری برای شبیه سازی و مدلسازی مبتنی بر عامل در تجزیه و تحلیل به اشتراک گذاری دانش امنیت اطلاعات. *مدیریت دانش سازمانی، ۵*(۱۸)، ۱۵۱-۱۹۹.

میرمحمدی، سیدمحمد؛ کریمی، محمدرضا؛ جوان جعفری، احمد. (۱۳۹۵). نقش میانجی انگیزش درونی در رابطه بین توانمندسازی ساختاری و پذیرش سیاست‌های امنیتی. *اولین کنفرانس بین‌المللی تحولات نوین در مدیریت، اقتصاد و حسابداری، تهران.*

نصیری ولیک بنی، فخرالسادات؛ محمدی، محمدفائق؛ باقری، سمیرا؛ باقری، پریسا. (۱۳۹۳). ارزیابی اثرات فناوری اطلاعات و ارتباطات بر امنیت روانی کارکنان مورد مطالعه سایت اداری سنندج. *کنفرانس بین‌المللی علوم رفتاری و مطالعات اجتماعی، تهران.*

هومن، حیدرعلی. (۱۳۹۷). مدل‌یابی معادلات ساختاری با کاربرد نرم‌افزار لیزرل. چاپ هشتم. *تهران، سمت.*

References

Abd Latif, S. F., Sulaiman, N. S., Abd Aziz, N. S., Yacob, A., & Nasir, A. (2025). Development of Cybersecurity Awareness Model Based on Protection Motivation Theory (PMT) for Digital IR 4.0 in Malaysia. *International Journal of Advanced Computer Science & Applications*, *16*(3).

Alshammari, M. M., & Al-Mamary, Y. H. (2025). Bridging Policy and Practice: Integrated Model for Investigating Behavioral Influences on Information Security Policy Compliance. *Systems*, *13*(8), 630.

Ashenden, D. (2018). In their own words: employee attitudes towards information security. *Information & Computer Security*, *26*(3), 327-337.

Chae, S.-S. (2025). The mediating effect of coping on the relationship between perceived risks and threats and the psychological well-being of hotel frontline employees. *Journal of Hospitality and Tourism Studies, 2*(113), 31–45. https://doi.org/10.31667/jhts.2025.02.113.31

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of management information systems*, *31*(2), 285-318.

Gabaldon, J., Niranjan, S., Hawkins, T. G., McBride, M. E., & Savitskie, K. (2024). Analyzing Protection Motivation Theory and Cognitive Failures in Texting While Driving Behavior Among Young Drivers. *Applied Cognitive Psychology*, *38*(6), e4252.

Goh, Z. H., Hou, M., & Cho, H. (2022). The impact of a cause–effect elaboration procedure on information security risk perceptions: a construal fit perspective. *Journal of Cybersecurity*, *8*(1), tyab026.

Gupta, S., & Bostrom, R. P. (2019). A revision of computer self-efficacy conceptualizations in information systems. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *50*(2), 71-93.

Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. (2019). Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences*, *50*(2), 245-284.

Kranz, J., & Haeussinger, F. (2014). Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior.

Mady, A., Gupta, S., & Warkentin, M. (2023). The effects of knowledge mechanisms on employees' information security threat construal. *Information Systems Journal*.

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203-1230.

Merhi, M. I., & Midha, V. (2012). The impact of training and social norms on information security compliance: A pilot study. Information Systems Journal, 33(4), 790–841.

Mou, J., Cohen, J. F., Bhattacherjee, A., & Kim, J. (2022). A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach. *Journal of the Association for Information Systems*, *23*(1), 196-236.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect

organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442-451.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *computers & security*, *56*, 70-82.

Shiau, W. L., Wang, X., & Zheng, F. (2023). What are the trend and core knowledge of information security? A citation and co-citation analysis. *Information & Management*, *60*(3), 103774.

Singh, A. (2025). From Past to Present: The Evolution of Data Breach Causes (2005–2025). *LatIA*, *3*, 333-333.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.

Tang, Z., Miller, A. S., Zhou, Z., & Warkentin, M. (2021). Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations. *Government Information Quarterly*, *38*(2), 101572.

Teng, M. F., & Zhang, L. J. (2024). Ethnic minority multilingual young learners' longitudinal development of metacognitive knowledge and breadth of vocabulary knowledge. *Metacognition and Learning*, *19*(1), 123-146.

Torabi, Z. A., Pourtaheri, M., Hall, C. M., Sharifi, A., & Javidi, F. (2023). Smart tourism technologies, revisit intention, and word-of-mouth in emerging and smart rural destinations. *Sustainability*, *15*(14), 10911.

Tran, D. V., Nguyen, P. V., Vrontis, D., Nguyen, S. T. N., & Dinh, P. U. (2024). Unraveling influential factors shaping employee cybersecurity behaviors: an empirical investigation of public servants in Vietnam. *Journal of Asia Business Studies*, *18*(6), 1445-1464.

Tran, D. V., Nguyen, P. V., Vrontis, D., Nguyen, S. T. N., & Dinh, P. U. (2024). Unraveling influential factors shaping employee cybersecurity behaviors: an empirical investigation of public servants in Vietnam. *Journal of Asia Business Studies*, *18*(6), 1445-1464.