J. SLIS, 17(4): 21-45, Winter 2025 slis.scu.ac.ir

Shahid Chamran University of Ahvaz

Journal of Studies in Library and Information Science
(*JSLIS*)

https://doi.org/10.22055/slis.2026.47681.1971

Research Paper

The effect of organizational factors on cyber security awareness with the mediating role of information security knowledge sharing attitude

Siroos Azizyan[1], Farshad Parhamnia[2*]

1. MBA Student in Information Systems and Information Technology, Department of Business Management, Kermanshah Branch, Islamic Azad University, Kermanshah, Iran.
2. Associate Professor, Department of Knowledge and Information Science, Kermanshah Branch, Islamic Azad University, Kermanshah, Iran.

Article Info.

Received: March 8, 2025 **Accepted**: August 25, 2025

Abstract

Background and Objectives: Cybersecurity awareness is essential for organizational resilience because employees' knowledge, attitudes, and routine actions can either strengthen or weaken the protection of information assets. This issue is particularly important in banks, where financial data and digital services make the consequences of security incidents especially serious. Previous research suggests that organizational culture, formal information security policies, and organizational support and training may shape employees' security-related behavior. These factors may also influence cybersecurity awareness indirectly by improving employees' attitudes toward sharing information security knowledge. However, the combined effects of these organizational factors and the mediating role of knowledge-sharing attitudes have received limited attention in Iranian banking. Therefore, this study examined the effects of organizational culture, organizational policy, and organizational support and training on employees' cybersecurity awareness, with attitude toward information security knowledge sharing as the mediating variable.

Methodology: This applied study used a descriptive-survey design. The statistical population consisted of 270 employees working in branches of Agricultural Bank in Kermanshah, Iran. The study described the sampling procedure as simple random sampling, and the sample size was estimated at 147 using Cochran's formula. Questionnaires were distributed and collected in person at employees' workplaces; 126 usable questionnaires were included in the final analysis. The instrument comprised 22 items measuring five constructs: organizational culture (six items), organizational policy (three items), organizational support and training (four items), attitude toward information security knowledge sharing (four items), and cybersecurity awareness (five researcher-developed items). Items for the first four constructs were adapted from Chen et al. (2015), Safa and Von Solms (2016), and Ma (2022). Face validity was assessed by four experts. Content validity was then examined by eight experts using the content validity ratio and content validity index; the final 22 items met the stated acceptance thresholds. Descriptive statistics were used to summarize the data, and partial least squares structural equation modeling was performed in SmartPLS to evaluate the measurement and structural models. The reported factor loadings, Cronbach's alpha coefficients, composite reliability values, average variance extracted values, and discriminant-validity results supported the adequacy of the measurement model.

Findings: Organizational culture did not have a significant effect on attitude toward information security knowledge sharing ($\beta = 0.057$, $t = 0.625$, $p = 0.532$). In contrast, organizational policy had a positive and significant effect on knowledge-sharing attitude ($\beta = 0.367$, $t = 4.064$, $p < 0.001$), as did organizational support and training ($\beta = 0.481$, $t = 6.392$, $p < 0.001$). Attitude toward information security knowledge sharing also had a positive and significant effect on cybersecurity awareness ($\beta = 0.496$, $t = 6.020$, $p < 0.001$). The indirect effect of organizational policy on cybersecurity awareness through knowledge-sharing attitude was significant ($\beta = 0.182$, $t = 3.444$, $p = 0.001$), and the corresponding indirect effect of organizational support and training was also significant ($\beta = 0.238$, $t = 4.436$, $p < 0.001$). The indirect effect of organizational culture was not significant ($\beta = 0.028$, $t = 0.595$, $p = 0.552$). The structural model explained 67.2% of the variance in attitude toward information security knowledge sharing and 24.6% of the variance in cybersecurity awareness. Predictive-relevance values were 0.430 and 0.173, respectively. The reported model-fit indices (SRMR = 0.062 for the saturated model and 0.063 for the estimated model; NFI = 0.815) indicated an acceptable fit, while the reported overall goodness-of-fit value was 0.612.

Discussion: The findings indicate that formal information security policies and tangible organizational support and training are more influential than general organizational culture in shaping employees' willingness to share security-related knowledge. In turn, a favorable knowledge-sharing attitude is associated with greater cybersecurity awareness and transmits part of the effects of policy, support, and training to awareness. The nonsignificant cultural path suggests that broad organizational values alone may be insufficient unless they are translated into clear rules, accessible guidance, practical training, and visible managerial support. Banks should therefore develop and clearly communicate information security policies, provide continuous skills-based cybersecurity training, establish accessible advisory channels for reporting and resolving security problems, and encourage employees to exchange experiences about threats and protective practices. Because the data were collected from employees of one bank in one city and at a single point in time, the findings should be generalized cautiously. Future studies could test the model in other organizational settings and use longitudinal designs to examine whether improvements in policy implementation, training, and knowledge sharing produce changes in cybersecurity awareness.

Keywords: Knowledge sharing; Cybersecurity awareness; Information security; Organizational culture; Organizational policy; Organizational support and training.

***Corresponding author:** Email: farshad.parhamnia@iau.ac.ir

How to Cite: Azizyan, S., & Parhamnia, F. (2025). The effect of organizational factors on cybersecurity awareness with the mediating role of information security knowledge sharing attitude. *Journal of Studies in Library and Information Science*, 17(4), 21-45. https://doi.org/10.22055/slis.2026.47681.1971

Authors retain the copyright and full publishing rights.
Published by Shahid Chamran University of Ahvaz. This article is an open access article licensed under the Creative Commons Attribution 4.0 International (CC BY 4.0)

فصلنامه
مطالعات کتابداری و علم اطلاعات. سال ۱۷، شماره ۴، زمستان ۱۴۰۴

مقاله پژوهشی

تأثیر عوامل سازمانی مؤثر بر آگاهی از امنیت سایبری با نقش میانجی‌گری نگرش به اشتراک‌گذاری دانش امنیت اطلاعات

سیروس عزیزیان[۱]، فرشاد پرهام‌نیا[۲*]

۱. دانشجوی کارشناسی ارشد رشته مدیریت کسب و کار- سیستم‌های اطلاعاتی و فناوری اطلاعات، واحد کرمانشاه، دانشگاه آزاد اسلامی، کرمانشاه، ایران.
۲. دانشیار گروه علم اطلاعات و دانش‌شناسی، واحد کرمانشاه، دانشگاه آزاد اسلامی، کرمانشاه، ایران

اطلاعات مقاله

تاریخ دریافت: ۱۴۰۳/۱۲/۱۸ **تاریخ پذیرش:** ۱۴۰۴/۰۶/۰۳

چکیده

هدف: بررسی عوامل سازمانی موثر بر آگاهی از امنیت سایبری با نقش میانجی‌گری نگرش به اشتراک گذاری دانش امنیت اطلاعات کارکنان شُعب بانک‌های کشاورزی شهر کرمانشاه بود.

روش‌شناسی: روش پژوهش حاضر از نظر هدف، کاربردی از نوع توصیفی- پیمایشی است. حجم نمونه برابر با ۱۲۶ نفر از کارکنان بودند. ابزار گردآوری داده‌ها با استفاده از پرسشنامه و در قالب پنج متغیر شامل فرهنگ سازمانی، خط و مشی سازمانی و پشتیبانی و آموزش به عنوان متغیرهای مستقل و متغیر نگرش به اشتراک‌گذاری دانش امنیت اطلاعات و آگاهی از امنیت سایبری به عنوان متغیرهای وابسته میانجی و ملاک بود. جهت تحلیل داده‌ها از نرم‌افزار SPSS و روش حداقل مربعات جزئی با نرم‌افزار Smart-PLS استفاده گردید.

یافته‌ها: یافته‌های پژوهش نشان داد که فرهنگ سازمانی اثر معناداری بر متغیر نگرش به اشتراک‌گذاری دانش امنیت اطلاعات نداشت. اما خط و مشی سازمانی و پشتیبانی سازمانی اثر معناداری بر متغیر نگرش به اشتراک‌گذاری دانش امنیت اطلاعات داشتند. همچنین متغیرهای خط و مشی سازمانی و پشتیبانی سازمانی با میانجی‌گری بر نگرش به اشتراک گذاری دانش امنیت اطلاعات و بر آگاهی از امنیت سایبری اثر معناداری داشت. اما متغیر فرهنگ سازمانی با میانجی‌گری بر نگرش به اشتراک‌گذاری دانش امنیت اطلاعات و بر آگاهی از امینت سایبری اثر معناداری نداشت.

نتیجه‌گیری: به طورکلی سازمان‌ها جهت تقویت آگاهی از امینت سایبری نیازمند برنامه‌ریزی و آموزش‌های لازم به منظور تدوین سیاست‌های امنیت سایبری می‌باشند. همچنین ضرورت دارد که به متغیرهای خط و مشی سازمانی، پشتیبانی و آموزش سازمانی و اشتراک گذاری دانش امنیت اطلاعات توجه ویژه‌ای داشته باشند.

کلیدواژه‌ها: *آگاهی از امنیت سایبری، اشتراک‌گذاری دانش امنیت اطلاعات، پشتیبانی و آموزش سازمانی، خط و مشی سازمانی، فرهنگ سازمان.*

***نویسنده مسئول**
ایمیل: farshad.parhamnia@iau.ac.ir

مقدمه و بیان مسئله

امروزه نقش و اهمیت اطلاعات در جوامع و حساسیت فرایندهای جمع‌آوری، ثبت و انتشار اطلاعات، دگرگونی بنیادینی را در ساختار مناسبات و ارتباطات جوامع ایجاد کرده است و همین امر، موجب ایجاد تهدیدها و نگرانی‌های جدید مبتنی بر اطلاعات شده است که مقولهٔ رفتارهای پرخطر دربارهٔ اطلاعات از آن جمله است. از طرفی، حملات و تهدیدات سایبری به مراتب پیچیده‌تر و از طرفی مخرب‌تر از گذشته شده‌اند (Taghipoor and Esmaeili, 2019). شولتز (Schultz, 2005) به این نکته اشاره می‌کند که تغییرات سریع در رایانه و فناوری اطلاعات به طور مستمر خطرات جدیدی را برای امنیت دارایی‌های اطلاعاتی ایجاد می‌کند (AlHogail, 2015). در عصر حاضر انفجار اطلاعات و فشارهای آن، سازمان‌ها را به سرمایه‌گذاری هنگفت در امنیت اطلاعات سوق می‌دهد تا اطمینان حاصل شود که تصمیمات فناوری اطلاعات با اهداف تجاری و مدیریت ریسک‌ها همسو هستند (Alzahrani & Seth, 2021). پیشرفت در فناوری‌ها و خدمات مبتنی بر وب با سرعت قابل توجهی در سراسر جهان در حال انجام است. با این حال، امنیت اطلاعات همچنان یک مسئله رایج در میان متخصصین و همچنین کاربران است. شرکت‌ها و مشتریان الکترونیکی نگران حملات سایبری هستند و در نتیجه، مایلند خطر امنیت اطلاعات را به حداقل برسانند (Safa and Ismail, 2013). از سویی، (Diesch, Pfaff & Krcmar, 2020) بیان می‌کنند که انفجار اطلاعات و فشارها، سازمان‌ها را به سرمایه‌گذاری هنگفت در امنیت اطلاعات سوق می‌دهد تا اطمینان حاصل شود که تصمیمات فناوری اطلاعات با اهداف تجاری و مدیریت ریسک‌ها هماهنگ است.

یکی از مفاهیمی که امروزه بایستی به آن پرداخته و از اهمیت خاصی در دنیای فناوری اطلاعات دارد، موضوع امنیت اطلاعات است. در این راستا الحسنا و ادجی-کوای (Alhassana & Adjei-Quaye, 2017) بیان می‌کنند که مطالعه امنیت اطلاعات دارای مفاهیم و موضوعات بسیار زیادی است که هر متخصص فناوری اطلاعات باید آن را داشته باشد. دانش و مهارت‌های مربوط به امنیت اطلاعات تنها چند مورد است که برای همه کسانی که در بخش فناوری اطلاعات درگیر هستند ضروری است.

امروزه به دلیل افزایش چشمگیر تهدیدات امنیت اطلاعات و گسترش مداوم رویه‌ها و مقررات برای امنیت اطلاعات، امنیت اطلاعات در کسب و کارها و به طور کلی در بخش تجاری اهمیت فزاینده‌ای پیدا کرده است. شرکت‌ها و مؤسسات منابع قابل توجهی را مصرف می‌کنند که حاوی تهدیداتی است که سیستم‌های اطلاعاتی آن‌ها را تهدید می‌کند. آن‌ها مجموعه‌ای از نرم‌افزارهای ضدجاسوسی، افزار/ضد ویروس، سیستم‌های تشخیص نفوذ و پیشگیری، فایروال‌ها و نرم افزارهای فیلتر محتوا را برای ایمن‌سازی سیستم‌های اطلاعاتی خود به کار می‌برند. با این حال، شکست و خطاهای انسانی ممکن است موانع زیادی در تأمین امنیت یک شرکت یا سازمان ایجاد کند (Tamjidyamcholo, 2013). با این وجود، امنیت اطلاعات همچنان یک نگرانی مهم برای کاربران و سازمان‌ها است. فناوری نمی‌تواند صرفاً یک محیط امن برای اطلاعات را تضمین کند. علاوه بر جنبه‌های تکنولوژیکی، بایستی جنبه‌های انسانی امنیت اطلاعات نیز در نظر گرفته شود. عدم آگاهی از امنیت اطلاعات، جهل، سهل انگاری، بی‌تفاوتی، شیطنت و مقاومت ریشه اشتباهات کاربران را تشکیل می‌دهد (Safa, Von Solms & Furnell, 2016) این درحالی است که رشد تصاعدی شیوه‌های مدیریت امنیت اطلاعات به دلیل نیاز صنعت فناوری اطلاعات برای مقابله آسان‌تر با کیفیت و قابلیت اطمینان کسب‌وکارهای بزرگ انجام شده است (Diesch, Pfaff & Krcmar, 2020). بنابراین، آگاهی از امنیت اطلاعات به حالتی از آگاهی گفته می‌شود که در آن کاربر به طور ایده آل به قوانین متعهد است، توانایی‌های بالقوه را تشخیص، اهمیت مسئولیت‌ها را درک و بر اساس آن عمل می‌کند. علیرغم تعداد موارد رخ داده در نقض امنیت اطلاعات، به ویژه در مؤسسه دانش‌بنیان که ناشی از عدم تمایل کاربر به رعایت دستورالعمل‌های امنیتی است، چنین اقدام مؤثری باید برای پیش‌بینی تأثیر منفی

صورت گیرد. بنابراین توجه بیشتر به درک نقش فردی، نهادی و محیطی برای بهینه‌سازی در افزایش آگاهی امنیت اطلاعات ضروری است (Ahlan, Lubis & Lubis, 2015).

یکی از کارهای مؤثری که یک کارمند می‌تواند برای ایجاد بهبود و توسعه سازمان انجام دهد، آگاهی از تهدیدات سایبری و امنیت سایبری است. امروزه، با توجه به افزایش خطر تهدیدات سایبری و پیامدهای شدیدی که توسط افراد یا سازمان‌ها به خصوص دشمنان انجام می‌شود، مدیریت مقابله با این تهدیدات برای حفاظت و امنیت اطلاعات کاملاً ضروری است. این وضعیت در بین بانک‌ها به دلیل ماهیت مالی و حساسی که دارند نیز به امری حیاتی تبدیل شده است. با اینکه در خصوص مقابله و دفع تهدیدات سایبری در بانک‌ها، سازمان‌ها و شرکت‌های کشور به صورت مستمر انجام و یا در حال انجام است و در این زمینه نیز به نتایجی دست یافته‌اند. ولی با توجه به ماهیت فناوری اطلاعات و اینترنت این وضعیت کافی نیست و لازم است کارکنان و مدیران اجرایی بانک‌ها نسبت به این تهدیدات، آگاهی بیشتری از تهدیدات و امنیت سایبری داشته باشند. با این حال، به نظر می‌رسد عواملی چند می‌تواند بر آگاهی از امنیت سایبری کارکنان نقش اساسی داشته باشد. به نظر می‌رسد این عوامل می‌تواند در قالب متغیرهای سازمانی شامل فرهنگ سازمانی، خط و مشی سازمانی و پشتیبانی و آموزش سازمانی اشاره کرد. همچنین این متغیرها می‌توانند با میانجی‌گری اشتراک‌گذاری دانش امنیت اطلاعات بر آگاهی امنیت سایبری نقش مهمی را ایفا کنند. طی بررسی‌های بعمل آمده در پایگاه‌های اطلاعاتی مشخص گردید که پژوهش مستقلی در خصوص عوامل سازمانی مؤثر شامل فرهنگ سازمانی، خط و مشی سازمانی و پشتیبانی و آموزش سازمانی که با میانجی‌گری نگرش به اشتراک‌گذاری دانش امنیت اطلاعات بر آگاهی از امنیت سایبری منتشر شده باشد، یافت نشد. این خلاء پژوهشی موجب شد که در این موضوع پژوهشی انجام شود. بنابراین با توجه به اهمیت موضوع برای بانک‌ها این مطالعه به دنبال این سوال اصلی است که عوامل سازمانی مؤثر با میانجی‌گری نگرش به اشتراک‌گذاری دانش امنیت اطلاعات می‌تواند بر آگاهی از امنیت سایبری کارکنان بانک کشاورزی شهر کرمانشاه اثر معناداری داشته باشد؟

مبانی نظری و پیشینه پژوهش

عوامل سازمانی شامل همه عناصر، عوامل و شرایط فیزیکی و غیرانسانی سازمانی است که با نظم، قاعده، قالب، پوسته و بدنه و یا هیکل فیزیکی و مادی سازمان را می‌سازد (Mirzaei Ahranjani, 1998). بنابراین وقتی بحث از عوامل سازمانی به میان می‌آید شامل خیلی از متغیرها می‌باشد که در درون یک سازمان رخ می‌دهد. به طور کلی عوامل سازمانی به خط مشی‌های مدیریتی، محیط کار، حجم کار و جنبه‌های دیگر محیط کار در یک سازمان است که می‌تواند بر روی عملکرد کارکنان آن سازمان تأثیر بسزایی داشته باشد. ولی برخی مواقع منجر به ایجاد خطای انسانی نیز می‌گردد و در نتیجه تهدیدات امنیت اطلاعات و یا تهدیدات سایبری ایجاد خواهد شد. در این پژوهش سه عامل مهم که نقش کلیدی در آگاهی از امنیت سایبری در برابر تهدیدات سایبری دارند شامل فرهنگ سازمانی، خط و مشی سازمانی و پشتیبانی و آموزش سازمانی است که در اینجا به اختصار در مورد آن ها بحث می‌شود:

فرهنگ سازمانی

فرهنگ به عنوان مجموعه‌ای از درک مشترک که در الگوهای مشترک کنش و معنا، مانند زبان مشترک بیان می‌شود، می‌توان مفهوم سازی کرد. تنگ، لی و زنگ (Tang, Li & Zhang, 2016) اظهار کردند که هر سازمانی فرهنگ خاصی دارد که از مجموعه‌ای از مفروضات، ارزش‌ها و هنجارها تشکیل شده و فعالیت‌های درون یک سازمان را هدایت می‌کند. در زمینه امنیت اطلاعات، فرهنگ حیاتی است و تحقیقات ثابت کرده است که بر امنیت اطلاعات تأثیر دارد (Mejias, 2012; Van Niekerk & Von Solms, 2010). هلریگل، اسلوکم و وودمن (Hellriegel, Slocum & Woodman, 1998) نیز در این رابطه بیان می‌کنند

که فرهنگ سازمانی در جایی ایجاد می‌شود که مدیران، چشم‌انداز و استراتژی سازمان را توسعه می‌دهند. رفتار کارکنان با هدایت چشم‌انداز، استراتژی و سیاست‌ها آشکار می‌شود. با گذشت زمان، یک فرهنگ سازمانی پدیدار می‌شود که دیدگاه و استراتژی و همچنین تجربیاتی که کارکنان هنگام اجرای آنها داشته‌اند را در بر می‌گیرد (Da Veiga, 2016). به طور کلی، فرهنگ امنیت اطلاعات شامل کلیه اقدامات اجتماعی–فرهنگی است که از اقدامات امنیتی فنی پشتیبانی می‌کند (Schlienger & Teufel, 2003). فرهنگ امنیت اطلاعات به عنوان راهی برای انجام کارها پیرامون امنیت اطلاعات، از جمله ایجاد محیطی که نگرش‌ها، ارزش‌ها و باورهای امنیتی مشترک را در یک سازمان تقویت و پرورش می‌دهد، تعریف می‌شود (Van Niekerk and Von Solms, 2010; Chen et al., 2015). دی ویگا و اولاف (Da Veiga & Eloff, 2010) و ویلسون و هش (Wilson & Hash, 2003) بیان می‌کنند که برای موفقیت مدیریت امنیت اطلاعات در یک سازمان، فرهنگ امنیت اطلاعات مجموعه‌ای از نیروهای آشکار و یا ضمنی برای شکل دادن نگرش و رفتار کارکنان نسبت به امنیت اطلاعات در بلند مدت است. تحت تأثیر فرهنگ امنیتی، کارمندان طرز فکر و رفتارهای امنیت اطلاعات را به شیوه‌ای طبیعی و بدیهی از خود نشان می‌دهند (Chen et al., 2015). بنابراین با توجه به مطالب فوق می‌توان این فرضیه را مطرح کرد که فرهنگ سازمانی با میانجی‌گری نگرش به اشتراک گذاری دانش امنیت اطلاعات بر آگاهی از امنیت اطلاعات اثر معناداری دارد.

خط و مشی سازمانی

سیاست‌های امنیتی، نگرش‌ها و رفتارهای مطلوب را نسبت به امنیت اطلاعات و پیامدهای نقض خط مشی‌ها توسط کارکنان ارتباط برقرار می‌کنند و سعی می‌کنند رفتارها را نسبت به امنیت اطلاعات اصلاح کنند (Straub et al., 2004; Chen et al., 2013). خط مشی امنیت اطلاعاتی که توسط سازمان ها به افراد ارائه داده می شود که در صورت داشتن مسائل امنیتی خاص، چه اقداماتی بایستی توسط افراد انجام شده و همچنین چگونه با منابع اطلاعاتی و فناوری سازمان خود تعامل بوجود آورند (Whitman, 2008). نیاز به خط مشی امنیت اطلاعات یک سازمان وجود دارد، این نباید صرفاً یک برنامه عملیاتی، به عنوان مثال، هدف، کاربرد، اهمیت و فعالیت های آن را بیان کند. مهم‌تر از همه، سازمان‌ها همچنین باید مستند کنند که چه کسی در نهایت مسئول اجرای دستور کار امنیتی در سراسر شرکت است (Allen et al., 2015). همه پرسنل درون سازمان باید در آموزش‌های مناسب در مورد خط مشی امنیت اطلاعات و انتظارات امنیتی سازمان، همسو با نقش های عملکردی آنها ارائه شوند. به عنوان مثال، خط مشی استفاده از اینترنت شرکتی باید به شیوه ای واضح ابلاغ شود، خوانده شود، درک شود و توسط همه پرسنل سازمان تأیید شود، در حالی که یک خط مشی خاص نقش مانند خط مشی مدیریت نرم افزار سازمانی باید شامل همه موارد مرتبط باشد. همچنین برای سازمان‌ها ضروری است که انتشار خط‌مشی‌ها و رویه‌ها را از طریق تأیید صلاحیت کارکنان پیگیری کنند، زیرا این امر به ارائه ورودی ارزشمند در اجرای سیاست‌ها و فرآیندهای آموزشی کمک می‌کند (Alhassana & Adjei-Quaye, 2017). بنابراین با توجه به مطالب فوق این پژوهش به دنبال آزمون این فرضیه است که خط و مشی سارمانی با میانجی‌گری نگرش به اشتراک گذاری دانش امنیت اطلاعات بر آگاهی از امنیت سایبری اثر معناداری دارد.

پشتیبانی و آموزش سازمانی

حمایت سازمانی به کارکنان و تعهد عاطفی کارکنان در یک سازمان اشاره دارد. باورهای جهانی در مورد میزانی که یک سازمان سهم کارکنان را به رسمیت می‌شناسد و برای آن‌ها ارزش قائل است و به رفاه آن‌ها توجه می‌کند (Shropshire et al., 2015). از طرفی، بر اهمیت حمایت سازمانی در تصمیم کاربران برای رعایت سیاست‌های امنیت اطلاعات تأکید شده است (Cavusoglu et al., 2015). مدیریت منابع کاربران و کارکنان سازمانی بر خلاف پرسنل امنیتی، مسئولیت مستقیمی در رابطه با امنیت ندارند. بنابراین صرف وجود آنها کمکی به امنیت نمی‌کند. کارکنان می‌توانند در صورتی به امنیت بیافزایند که سطح دانش

آنها، یعنی آگاهی از تهدیدات امنیتی و دانش در مورد اجتناب از آنها کافی باشد. آگاهی از امنیت اطلاعات اغلب به عنوان یک کنترل نامشهود برای امنیت اطلاعات در بین شاغلین شناخته می‌شود زیرا مکمل کنترل‌های فنی است (Cavusoglu et al., 2015). در پژوهش (Parsons et al. 2014) به این نتیجه دست یافتند که کمپین‌های آموزشی تأثیر مثبتی بر دانش کارکنان از خط مشی‌ها و رویه‌ها داشته است. پشیبانی سازمانی و آموزش مستمر کارکنان نقش مهمی در جلوگیری از تهدیدات سایبری خواهد داشت. با این حال، مؤثرترین وسیله برای دستیابی به امنیت سازمان، پرورش آگاهی و ارائه آموزش‌های امنیتی به کارکنان می‌باشد. برنامه‌های آگاهی امنیتی، کاربران را قادر می‌سازد تا نگرانی‌های امنیتی را شناسایی کرده و آنها را با تحریم‌های سازمانی که ممکن است در نتیجه نقص‌های امنیتی اعمال شود، آشنا کنند. آگاهی و آموزش در کنار هم به کاربران سازمانی این امکان را می‌دهد که در موقعیت بهتری برای جلوگیری از نقض امنیتی ناشی از سهل انگاری یا خطا و همچنین مواردی که ناشی از فعالیت‌های مخرب هستند، باشند (Cavusoglu et al., 2015). بنابراین با توجه به مطالب فوق این پژوهش بدنبال آزمون این فرضیه است که پشتیبانی و آموزش سارمانی با میانجی‌گری نگرش به اشتراک گذاری دانش امنیت اطلاعات بر آگاهی از امنیت اطلاعات اثر معناداری دارد.

نگرش به اشتراک‌گذاری دانش امنیت اطلاعات

پژوهشگرانی همانند کابررا و کابرر (Cabrera and Cabrera, 2002)، (Wang and Noe, 2010) و (Nielsen and Cappelen, 2014) بیان می‌کنند که علیرغم چندین تلاش برای تعریف اشتراک دانش، این موضوع همچنان به عنوان یک موضوع بحث برانگیز در بین دانشگاهیان و متخصصان و بسته به زمینه و دیدگاهی که در آن استفاده می‌شود، باقی مانده است (Al-Kurdi, El-Haddadeh& Eldabi, 2018). با این حال، اشتراک دانش روشی است که در آن رفتار افراد نسبت به توزیع و تبادل اطلاعات به دست آمده با انتقال این دانش به همکاران افزایش می‌یابد (Yesil, Koska & Büyükbese, 2013). در جایی دیگر، اشتراک دانش را تبادل متقابل مردم از تجزیه و تحلیل ذهنی و درک اطلاعات، نظرات و ایده ها برای بهبود ارتباطات و ایجاد دانش جدید تعریف شده است (Islam et al., 2013). برخی دیگر از پژوهشگران مانند (Yi, 2009) اشتراک گذاری دانش در محل کار را مجموعه ای از رفتارها توصیف می کند که شامل به اشتراک گذاری دانش مربوط به کار یک کارمند با کارمند دیگر با هدف دستیابی به اهداف سازمانی است. در نهایت (Akturan & Çekmecelioglu, 2016) تایید کردند که مبادله دانش متکی به تمایل اعضا برای به اشتراک گذاشتن داوطلبانه دانش کسب شده خود با دیگران علاوه بر شهروندی سازمانی است، در نتیجه ناگزیر دانش مشترک را به طور قابل توجهی القا می‌کند. بنابراین، اشتراک دانش امنیت اطلاعات رویکردی مؤثر برای افزایش سطح آگاهی است. کارشناسان در این زمینه با مشکلات مشابهی روبرو هستند و باید راه حل های مناسب ارائه دهند. جلوگیری از تکراری شدن توسعه راه حل های مشابه برای مشکلات مشابه با به اشتراک گذاری دانش منجر به جلوگیری از اتلاف وقت و هزینه می شود (Feledi, Fenz & Lechner, 2013). با این حال، فلورس و همکاران (Flores et al., 2014) بیان می‌کنند که به اشتراک گذاری دانش امنیت اطلاعات نقش مهمی در حوزه امنیت اطلاعات بازی می‌کند زیرا که این اشتراک دانش موجب افزایش آگاهی از امنیت اطلاعات می شود (Kiashmeshki & Daneshvar, 2022). بنابراین با توجه به مطالب فوق این پژوهش به دنبال آزمون این فرضیه است که نگرش به اشتراک گذاری دانش امنیت اطلاعات بر آگاهی از امنیت اطلاعات اثر معناداری دارد.

آگاهی از امنیت سایبری

هدف امنیت اطلاعات تضمین تداوم کسب و کار و محدود کردن تأثیر حوادث امنیتی به منظور به حداقل رساندن خسارات تجاری است (Von Solms & Van Niekerk, 2013). حتی در این دوره، تعدادی جرایم سایبری ثبت شد که شامل جاسوسی،

سرقت و هک بود (Warner, 2012). امنیت اطلاعات فرایند حفاظت از اطلاعات در مقابل کارهای غیرمجاز همچون دسترسی، افشا، اختلال، تغییرو یا تخریب می باشد (Kiashmeshki & Daneshvar, 2022). تعریف دقیق امنیت سایبری هنوز به طور فعال در جامعه علمی مورد بحث است. در تعریف آن سازمان بین‌المللی استاندارد (The International Organization for Standardization) و کمیسیون بین‌المللی الکتروتکنیکی (The International Electrotechnical Commission, 2012) امنیت سایبری را به عنوان حفاظت و حفظ محرمانه بودن، یکپارچگی و در دسترس بودن اطلاعات که یک دارایی در قلمرو فضای سایبری است تعریف شده است (Gcaza et al., 2017). کیم، چوی و هان (Kim, Choi & Han, 2019) در تعریف آگاهی از امنیت اطلاعات بیان می کنند که آگاهی از امنیت سایبری به عنوان دانش و درک کلی از مشکلات مربوط به امنیت اطلاعات و پیامدهای آنها و همچنین آنچه که برای رسیدگی به آنها باید انجام شود (Khan et al., 2023).

با این حال، امنیت سایبری با توجه به اطلاعاتی که در فضای سایبری به اشتراک گذاشته و افشا می شود، بسیار فراتر از مرزهای یک تجارت است. بنابراین، حتی اگر ارتباط نزدیکی بین امنیت اطلاعات و امنیت سایبری وجود دارد، جنبه هایی وجود دارد که خارج از محدوده امنیت اطلاعات قرار دارند (Von Solms & Van Niekerk, 2013). بر این اساس، آنها استدلال کردند که امنیت سایبری به عنوان «حفاظت از خود فضای سایبری، اطلاعات الکترونیکی، فناوری‌های اطلاعاتی و ارتباطاتی که از فضای سایبری پشتیبانی می‌کنند، و کاربران فضای سایبری در فضای شخصی، اجتماعی خود تعریف می‌شود. و ظرفیت ملی، از جمله هر یک از منافع آن‌ها، اعم از محسوس یا ناملموس که در برابر حملات ناشی از فضای سایبری آسیب‌پذیر هستند. بنابراین با توجه به مطالب فوق، این پژوهش به دنبال آزمون این فرضیه است که فرهنگ سازمانی، خط و مشی سازمانی و پشتیبانی سازمانی با میانجی‌گری نگرش به اشتراک گذاری دانش امنیت اطلاعات بر آگاهی از امنیت سایبری تأثیر مثبت و معناداری دارد

پیشینه پژوهش

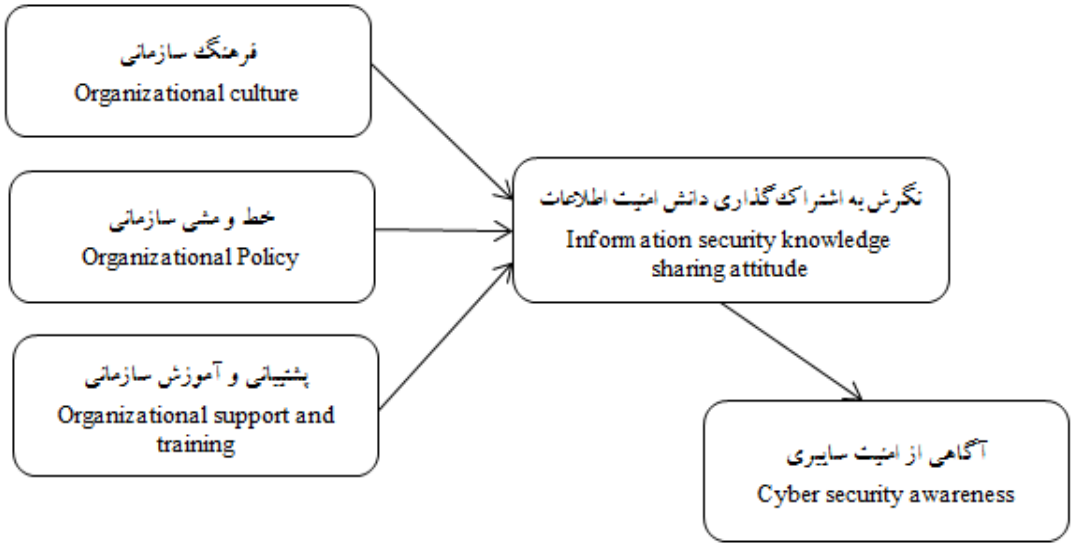
طی بررسی‌های بعمل آمده در منابع فارسی و خارجی، پژوهش‌های در خصوص عوامل سازمانی بر اشتراک گذاری دانش امنیت اطلاعات پرداخته شده است ولی پژوهشی اندکی تأثیر این عوامل بر آگاهی از امنیت سایبری انجام شده است. در اینجا به برخی از آن‌ها که قرابتی با متغیرهای این پژوهش دارند، اشاره می‌شود.

نتایج پژوهش (Parsons et al., 2014) نشان داد که کمپین‌های آموزشی تأثیر مثبتی بر دانش کارکنان از خط مشی‌ها و رویه‌ها داشته است. چن و همکاران (Chen et al., 2015) در مقاله ای با عنوان تأثیر برنامه های جامع امنیت اطلاعات بر فرهنگ امنیت اطلاعات بیان داشتند که آگاهی برنامه‌های SETA تأثیرات قابل‌توجهی بر فرهنگ امنیتی و آگاهی کارکنان از سیاست امنیتی سازمانی دارد و آگاهی از نظارت امنیتی نیز بر فرهنگ امنیتی تأثیر می‌گذارد. صفا و ون سولماز (Safa & Von Solms, 2016) در مقاله‌ای به بررسی مدل اشتراک دانش امنیت اطلاعات در سازمان ها پرداختند. نتایج این پژوهش حاکی از آن داشت که کسب شهرت و ارتقاء به عنوان انگیزه بیرونی و رضایت از کنجکاوی به عنوان انگیزه درونی بر نگرش کارکنان نسبت به اشتراک دانش امنیت اطلاعات تأثیر مثبت دارد. با این حال، رضایت از خود ارزشی بر نگرش اشتراک دانش امنیت اطلاعات تأثیر نمی‌گذارد. علاوه بر این، یافته‌ها نشان داد که حمایت سازمانی بر رفتار اشتراک دانش امنیت اطلاعات بیش از اعتماد تأثیر می گذارد. نتایج این تحقیق باید مورد توجه دانشگاهیان و دست اندرکاران حوزه امنیت اطلاعات باشد. داویگ (Da Veiga, 2016) در بررسی مقایسه فرهنگ امنیت اطلاعات کارکنانی که خط مشی امنیت اطلاعات را مطالعه نکرده اند نشان داده شده از طریق یک مطالعه تجربی پرداختند. یافته‌ها میانگین نمرات کلی فرهنگ امنیت اطلاعات و همچنین اظهارات فردی برای هر چهار ارزیابی نظرسنجی برای کارکنانی که خط مشی امنیت اطلاعات را مطالعه کرده بودند در مقایسه با کارکنانی که مطالعه نکرده بودند به طور قابل توجهی مثبت تر بود. فرهنگ کلی امنیت اطلاعات نیز از یک ارزیابی به ارزیابی بعدی بهبود یافته است. اوبیتاده (Obitade, 2019)

در مقاله‌ای با عنوان تجزیه و تحلیل داده‌های بزرگ: پیوندی بین قابلیت های مدیریت دانش و حفاظت برتر سایبری پرداختند. نتایج این پژوهش حاکی از آن داشت که سازمان‌ها برای استفاده مؤثر از منابع اینترنت به قابلیت‌های تجزیه و تحلیل داده‌های پیشرفته نیاز دارند، که به آنها اجازه می‌دهد به حوادث سایبری با سرعت و چابکی پاسخ دهند که در نهایت در حفاظت سایبری برتر از دارایی‌های اطلاعاتی ارزشمند انباشته می‌شود. نتایج همچنین مفاهیم مفیدی را برای تحقیقات و اقدامات مدیریتی ارائه می‌دهد. ما (Ma, 2022) در پژوهشی به بررسی رفتارهای امنیت اطلاعات متخصصان IS در سازمان های فناوری اطلاعات چین برای حفاظت از امنیت اطلاعات پرداخت. نتایج این پژوهش نشان داد که نگرش های امنیت اطلاعات و هنجارهای ذهنی، به عنوان اجزای تشکیل دهنده نظریه رفتار برنامه ریزی شده، به طور قابل توجهی بر رفتارهای حفاظتی امنیت اطلاعات تأثیر می گذارد. ارزیابی های مقابله ای (خودکارآمدی و هزینه پاسخ) و ارزیابی های تهدید (حساسیت تهدید و شدت تهدید) نظریه انگیزه حفاظت به طور قابل توجهی رفتارهای حفاظتی امنیت اطلاعات را پیش بینی می کرد. و تعهد سازمانی تأثیر مثبتی بر رفتارهای حفاظتی امنیت اطلاعات داشت. با این حال، رضایت شغلی و کنترل رفتاری درک شده به عنوان ساختاری از نظریه رفتار برنامه ریزی شده با رفتارهای امنیت اطلاعات مرتبط نبود. دیسچ و همکاران (Diesch et al., 2020) در پژوهشی به بررسی تأثیر شیوه‌های سازمانی بر عملکرد مدیریت امنیت اطلاعات پرداختند. نتایج پژوهش نشان داد که آموزش امنیتی، اشتراک دانش، آموزش امنیتی و دید امنیتی به طور قابل‌توجهی بر عملکرد امنیت اطلاعات تأثیر می‌گذارد. علاوه بر این، این مطالعه تأثیر قابل توجهی از آموزش امنیتی و اشتراک دانش بر اعتماد در سازمان را برجسته می کند. الزهرانی و ست (Alzahrani & Seth, 2021) در مطالعه‌ای به بررسی تأثیر شیوه‌های امنیتی سازمانی بر عملکرد مدیریت امنیت اطلاعات با پارامترهای بسیاری پرداختند. نتایج نشان داد که آموزش امنیتی، اشتراک دانش، آموزش امنیتی و دید امنیتی به طور قابل‌توجهی بر عملکرد امنیت اطلاعات تأثیر می‌گذارد. علاوه بر این، این مطالعه تأثیر قابل توجهی از آموزش امنیتی و اشتراک دانش بر اعتماد در سازمان را برجسته می‌کند. کارلسون و همکاران (Karlsson et al., 2022) در پژوهشی به بررسی ارتباط بین فرهنگ‌های سازمانی ادراک شده مختلف و انطباق با خط مشی امنیت اطلاعات در میان کارکنان یقه سفید پرداختند. نتایج نشان داد که فرهنگ‌های سازمانی با تمرکز داخلی به طور مثبتی با انطباق خط‌مشی امنیت اطلاعات کارکنان مرتبط است. به نظر می رسد تفاوت در فرهنگ سازمانی از نظر کنترل و انعطاف پذیری تأثیر کمتری داشته باشد. تجزیه و تحلیل نشان می دهد که یک شکل بوروکراتیک از فرهنگ سازمانی برای تقویت انطباق با خط مشی امنیت اطلاعات کارکنان بیشترین سود را دارد. آکتر و همکاران (Akter et al., 2023) به بررسی مفهوم سازی مجدد قابلیت آگاهی از امنیت سایبری در اقتصاد دیجیتال مبتنی بر داده پرداختند. نتایج این پژوهش حاکی از آن داشت که کارکنان (دانش، نگرش و یادگیری)، مدیریت (آموزش، فرهنگ و جهت‌گیری استراتژیک) و قابلیت‌های زیرساختی (تکنولوژی و حاکمیت داده) را به عنوان ابعاد موضوعی برای مقابله با چالش‌های آگاهی از امنیت سایبری نشان می‌دهد. شاه بهرامی و همکاران (Shah Bahrami, 2017) در مقاله‌ای به بررسی شناسایی و اولویت بندی پارامترهای تاثیرگذار بر سیستم مدیریت امنیت اطلاعات شعب تامین اجتماعی استان گیلان پرداختند. نتایج این پژوهش نشان داد که عوامل نرم شامل عوامل مدیریتی و فرهنگی/ اجتماعی نسبت به عوامل سخت شامل عوامل مالی و فنی/ فناورانه درسیستم مدیریت امنیت اطلاعات از اهمیت بیشتری برخوردار بوده و عوامل مدیریتی نسبت به سایر عوامل نرم و همچنین عوامل فنی/ فناورانه نسبت به سایر عوامل سخت دارای بیشترین اهمیت هستند. در نهایت پژوهش آذر و مهدی‌پور (Azar & Mahdavipur, 2022) نشان داد که عوامل درون سازمانی شامل امن‌سازی تجهیزات، شبکه‌ها، نرم افزارها، رصد و پایش رخدادهای سایبری و واکنش به موقع به آن‌ها و ارتقاء دانش سایبری کارکنان و عوامل برون سازمانی شامل تهدیدات سایبری انسان‌ساز و طبیعی، عوامل مؤثر بر امنیت سایبری تشکیل می‌دهند.

جمع‌بندی پیشینه‌ها نشان داد که مطالعات پیشین به گونه‌ای به صورت جزئی به آگاهی از امنیت اطلاعات اشاره کرده‌اند. این پژوهش‌ها به سه دسته یعنی پژوهش‌های مرتبط با برنامه‌های آموزشی، برنامه‌های جامع امنیت اطلاعات، آموزش امنیتی، دید

امنیتی، اشتراک دانش بر امنیت اطلاعات؛ دسته دوم، پژوهش‌های مرتبط با عوامل رفتاری همچون کسب شهرت و ارتقاء(انگیزه بیرونی و درونی) بر نگرش کارکنان نسبت به اشتراک دانش امنیت اطلاعات، رفتارها و نگرش‌های امنیت اطلاعات، نگرش و یادگیری کارکنان، و دسته سوم پژوهش‌هایی که به صورت جزئی به عواملی همچون فرهنگ سازمانی، فرهنگ امنیت اطلاعات، حمایت سازمانی، شیوه‌های سازمانی، شیوه‌های امنیتی سازمانی، عوامل مدیریتی و زیرساختی، درون سازمانی و برون سازمانی بر امنیت اطلاعات بودند. باید به این نکته توجه داشت که پژوهش‌های فوق دارای نقاط اشتراک بسیاری هستند. اما در خصوص عوامل سازمانی مؤثر بر آگاهی از امنیت سایبری با نقش میانجی نگرش به اشتراک گذاری دانش امنیت اطلاعات، پیشینه‌ای به صورت مستقل یافت نشد. لذا این مطالعه با بررسی عوامل سازمانی مؤثر بر آگاهی از امنیت سایبری که تاکنون توجه نسبتاً کمی به آن‌ها شده است، پرداخته می‌شود و ز نظر کمبود شکاف تحقیقاتی به مجموعه آگاهی از امنیت سایبری، تهدیدات سایبری و در نهایت امنیت اطلاعات کمک خواهد کرد. با توجه به مبانی نظری این مطالعه، مدل مفهومی بر اساس شکل ۱ ترسیم شد.



شکل ۱. مدل مفهومی پژوهش

Figure 1. The conceptual model of research

مطابق شکل ۱، چارچوب مدل شامل اثر بین عوامل سازمانی از جمله فرهنگ سازمانی، خط و مشی سازمانی و پشتیبانی و آموزش سازمانی بر نگرش به اشتراک‌گذاری دانش امنیت اطلاعات بر آگاهی از امنیت سایبری است.

روش‌شناسی پژوهش

روش پژوهش حاضر از نظر هدف کاربردی و بر اساس ماهیت، روش انجام کار، نحوه اجرا و گردآوری داده‌ها از نوع پژوهش‌های توصیفی- پیمایشی است. جامعهٔ آماری این مطالعه، تعداد ۲۷۰ نفر از کارکنان شُعب بانک کشاورزی شهر کرمانشاه بود. انتخاب شهر و جامعه آماری هدفمند بود. شهر کرمانشاه نهمین شهر پرجمعیت و یکی از کلان‌شهرهای معروف و قدیمی ایران است که دارای موقعیت استراتژیک و ژئوپلیتیک جغرافیایی و سیاسی و دارای جایگاه ارزشمند و مهمی در کشور می‌باشد. همچنین بانک کشاورزی با قدمت بیش از ۹۰ سال یکی از بانک‌های تخصصی کشور می باشد که در زمینه ارائه خدمات بانکی و حمایت از بخش کشاورزی و زیر بخش‌های آن پیشرو بوده و به عنوان یکی از اثرگذارترین بانک‌ها در رشد اقتصادی کشور محسوب می گردد. روش نمونه‌گیری در این پژوهش به صورت تصادفی ساده و از طرفی پرسشنامه در اختیار افرادی قرار گرفت که تمایل به تکمیل آن داشتند.

حجم نمونه بر اساس فرمول کوکران ۱۴۷ نفر بودند. ابزار گردآوری داده‌ها با استفاده از پرسشنامه استفاده شد. جهت توزیع و گردآوری داده‌ها محقق اول با حضور در محل کار کارکنان یعنی در شعب بانک کشاورزی شهر کرمانشاه انجام شد. در مجموع تعداد ۱۲۶ پرسشنامه بدون نقص انتخاب شدند. این پرسشنامه شامل ۵ متغیر و در ۲۲ سؤال می‌باشد که از پژوهش‌های پیشین اقتباس با تغییریاتی در آنها استفاده شد. متغیر فرهنگ سازمانی با شش سؤال از پژوهش (Chen et al, 2015) ، خط و مشی سازمانی با سه سؤال از پژوهش (Chen et al, 2015)، و پشتیبانی و آموزش سازمانی با ۴ سؤال از پژوهش (Safa & Von Solms, 2016)، متغیر نگرش به اشتراک گذاری دانش امنیت اطلاعات با ۴ سؤال از پژوهش (Safa & Von Solms, 2016) و پژوهش (Ma, 2022) ، و متغیر آگاهی از امنیت سایبری با ۵ سؤال به صورت محقق ساخته استفاده شد. لازم بذکر است دو متغیر نگرش به اشتراک گذاری دانش امنیت اطلاعات و متغیر آگاهی از امنیت سایبری به عنوان متغیرهای وابسته میانجی و وابسته ملاک هستند. به منظور بررسی روایی پژوهش از دو منظر روایی صوری و روایی محتوایی استفاده شد. ابتدا پرسشنامه با ۲۵ سوال در اختیار چهار نفر از خبرگانی که دارای کار پژوهشی و در مورد امنیت اطلاعات و تهدیدات سایبری شناخت داشتند، قرار گرفت. از آنان خواسته شد که در خصوص سوالات هر متغیر و مولفه از نظر تناسب یا عدم تناسب سؤالات با متغیرها، ابهام موجود در نگارش سوالات، وجود نارسایی در معانی کلمات و جملات را بیابند. در نهایت نظرهای آن‌ها در قالب تغییرات جزئی، ادغام سوالات با همدیگر و یا حذف سوالات در برخی از متغیرها در پرسشنامه اعمال شد. دوم، بعد از روایی صوری، پرسشنامه جهت محاسبه نسبت روایی محتوایی و شاخص روایی محتوایی در اختیار ۸ نفر از خبرگان قرار گرفت و از آنان خواسته شد که هر یک از سوالات به صورت "ضروری است"، "ضروری نیست ولی مفید است" و "ضرورتی ندارد" پاسخ دهند. پاسخ‌ها با جدول لاوشه (Lawshe, 1975) انطباق داده شد اعداد بالاتر از ۰/۷۵ مورد قبول واقع گردید. سپس جهت بررسی شاخص روایی محتوایی بر اساس شاخص روایی محتوایی والتز و باسل (Waltz and Basel, 1981) صورت گرفت. بدین منظور از خبرگان درخواست شد که در مورد هر یک از سوالات پرسشنامه بر اساس طیف لیکرت چهار گزینه‌ای ۱. غیرمرتبط ۲. تاحدودی مرتبط ۳. مرتبط، ۴ کاملاً مرتبط پاسخ دهند. بدین منظور امتیاز شاخص روایی محتوایی به وسیله مجموع امتیازات موافق برای هر آیتم رتبه ۳ و ۴ (بالاترین نمره) کسب کردند بر تعداد کل متخصصین محاسبه شد. بنابراین پذیرش سوالات بر اساس نمره شاخص روایی محتوایی بالاتر از ۰/۷۹ بود و در نهایت ۲۲ سؤال برای عوامل سازمانی مورد تأئید قرار گرفت. روش تجزیه و تحلیل داده‌ها با استفاده از آمار توصیفی و جهت بررسی مدل از روش حداقل مربعات جزئی و با استفاده از نرم افزار Smart-PLS استفاده شد.

یافته‌های پژوهش

بررسی وضعیت ویژگی‌های جمعیت‌شناختی پاسخگوان پرسشنامه نشان داد که از مجموع ۱۲۶ نفری که در این پژوهش شرکت کردند تعداد ۳۱ نفر معادل ۲۴/۶ درصد زن و تعداد ۹۵ نفر معادل ۷۵/۴ درصد مرد بودند. از نظر سن تعداد ۱ نفر بین ۱۵ الی ۲۰ سال با کمترین گروه سنی و تعداد ۳۴ نفر بین ۳۶ الی ۴۰ سال با بیشترین گروه سنی در این پژوهش بودند. از نظر تحصیلات پاسخگویان، تعداد ۸ نفر معادل ۶/۳ درصد دیپلم، ۸ نفر معادل ۶/۳ درصد کاردانی، ۵۷ نفر معادل ۴۵/۲ درصد کارشناسی و ۵۳ نفر معادل ۴۲/۱ درصد دارای مدرک کارشناسی ارشد به بالا بودند. از نظر سابقه خدمت پاسخگویان، تعداد ۱۱ نفر معادل ۸/۷ درصد دارای ۱ الی ۵ سال سابقه با کمترین تعداد و ۳۴ نفر معادل ۲۷ درصد دارای ۲۱ الی ۲۵ سال سابقه خدمتی بودند. در نهایت از نظر میزان تجربه و اطلاعات در خصوص تهدیدات سایبری مشخص شد که تعداد ۲۰ نفر معادل ۱۵/۹ درصد کمتر از حد متوسط دارای میزان تجربه و اطلاعات در خصوص تهدیدات سایبری بوده و تعداد ۱۰۶ نفر معادل ۸۴/۱ درصد از پاسخگویان بیشتر از حد متوسط به بالا دارای تجربه و اطلاعات در خصوص تهدیدات سایبری داشتند.

مدل‌سازی معادلات ساختاری

جهت بررسی روایی و پایایی پرسشنامه در متغیرهای عوامل رفتاری شامل حساسیت تهدید درک شده، شدت تهدید درک شده، آسیب پذیری درک شده، خودکارآمدی، هنجارهای ذهنی و انگیزی با استفاده از بارهای عاملی، آلفای کرونباخ، میانگین واریانس استخراج شده، و پایایی ترکیبی مورد آزمون قرار گرفت. برازش یک مدل اندازه‌گیری مربوط به بخشی از مدل کلی می‌باشد که شامل یک متغیر همراه با گویه‌های آن متغیر است. جهت برازش مدل اندازه‌گیری در روش حداقل مربعات جزیی از سه مورد شامل پایایی شاخص (آلفای کرونباخ و پایایی ترکیبی)، روایی همگرا (میانگین واریانس استخراج شده و بارهای عاملی به روش چرخش واریماکس) و روایی واگرا با استفاده از جذر میانگین واریانس استخراج شده متغیرهای مکنون مورد سنجش قرار می‌گیرد. نتایج این آزمون‌ها در جدول ۱ نشان داده شده است.

جدول ۱. بارهای عاملی (به روش چرخش واریماکس، آلفای کرونباخ، پایایی ترکیبی و میانگین واریانس استخراج شده)

Table 1. Factor loadings (Varimax rotation method, Cronbach's alpha, combined reliability and average variance extracted)

متغیرها	سؤالات	بارهای عاملی	آلفای کرونباخ	پایایی ترکیبی	میانگین واریانس استخراج شده
فرهنگ سازمانی Organizational culture	1	0.782	0.929	0.944	0.739
	2	0.860			
	3	0.862			
	4	0.883			
	5	0.900			
	6	0.866			
خط و مشی سازمانی Organizational Policy	7	0.894	0.846	0.907	0.765
	8	0.899			
	9	0.830			
پشتیبانی و آموزش سازمانی Organizational support and training	10	0.858	0.879	0.916	0.733
	11	0.873			
	12	0.871			
	13	0.823			
نگرش به اشتراک دانش امنیت اطلاعات Information security knowledge sharing attitude	14	0.825	0.879	0.917	0.735
	15	0.872			
	16	0.904			
	17	0.825			
آگاهی از امنیت سایبری Cyber security awareness	18	0.878	0.942	0.955	0.811
	19	0.917			
	20	0.872			
	21	0.929			
	22	0.906			

مطابق با جدول ۱، آلفای کرونباخ حاکی از آن دارد که تمامی ۵ متغیر دارای آلفای بالاتر از ۰/۷ بودند. آلفای کرونباخ یک معیار سنتی برای تعیین پایایی سازه‌ها است. روش حداقل مربعات جزیی معیار جدیدتری با عنوان پایایی ترکیبی که توسط ورتس و همکاران (۱۹۷۴) معرفی شده بکار می‌گیرد. مقدار این شاخص بایستی بالاتر از ۰/۷ باشد که نشان از پایداری درونی مناسب برای مدل‌های اندازه‌گیری را دارد. این شاخص در پژوهش حاضر بالاتر از ۰/۷ بوده که نشان‌دهنده برازش مناسب مدل‌های اندازه‌گیری مورد تأئید قرار گرفت (C.R.>0.7). ستون بعدی مربوط به میانگین واریانس استخراج شده است. Fornell &Laecker, (1981) پیشنهاد می‌کنند که میانگین واریانس استخراج شده باید بزرگتر از ۰/۵ باشد. میانگین واریانس استخراج شده در این مطالعه بین ۰/۷۳۲ تا ۰/۸۱۱ بود.

خروجی بعدی از معادلات ساختاری اجرای آزمون فورنل و لارکر برای بدست آوردن روایی واگرا بود. با توجه به اعتبار تمایز، طبق گفته (Fornell & Laecker, 1981)، جذر میانگین واریانس استخراج شده برای هر سازه باید از همبستگی‌های بین سازه با سایر سازه‌های مدل تجاوز کند. همانطور که در جدول ۲ نشان داده شده است.

جدول ۲. بررسی روایی واگر متغیرهای پژوهش

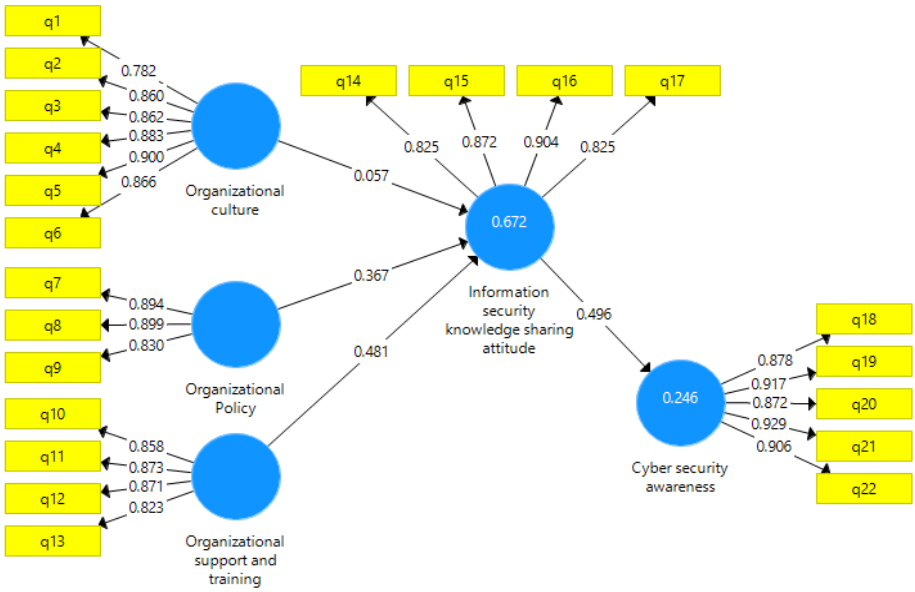
Table 2. Assessment of Discriminant Validity of the Research Variables

متغیرها Variables	1	2	3	4	5
1. آگاهی از امنیت سایبری Cyber security awareness	0.901				
2. نگرش به اشتراک گذاری دانش امنیت اطلاعات Information security knowledge sharing attitude	0.496	0.857			
3. فرهنگ سازمانی Organizational culture	0.364	0.672	0.860		
4. خط و مشی سازمانی Organizational Policy	0.343	0.728	0.777	0.875	
5. پشتیبانی و آموزش سازمانی Organizational support and training	0.416	0.762	0.687	0.659	0.856

مطابق جدول ۲، مقدار همبستگی میان شاخص‌ها با سازه‌های مربوط به خود از همبستگی میان آنها و سایر سازه‌ها بیشتر است. به عبارتی دیگر، مقدار جذر میانگین واریانس استخراج شده متغیرهای مکنون در که در خانه‌های موجود در قطر اصلی ماتریس قرار گرفته‌اند، از مقدار همبستگی میان آنان که در خانه‌های زیرین قطر اصلی ترتیب داده شده‌اند، بیشتر است، که این وضعیت حاکی از روایی واگرا مناسب مدل است. از این رو، با تجزیه و تحلیل نتایج مدل اندازه گیری، می‌توان نتیجه گرفت که داده‌ها برای برآورد معادلات ساختاری کافی هستند.

آزمون فرضیه‌ها با استفاده از روابط ساختاریافته خطی

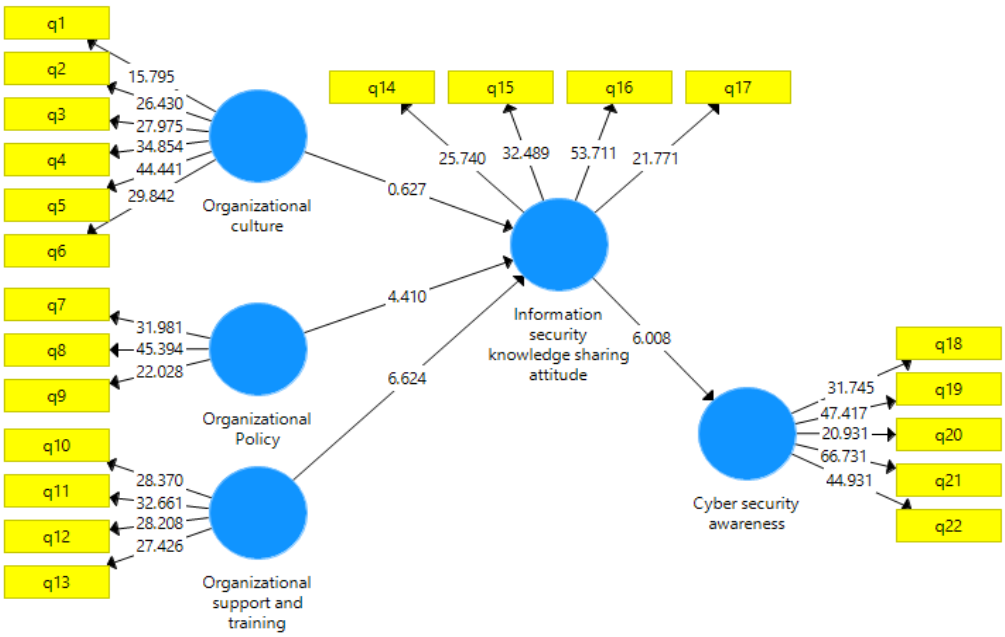
پس از بررسی مدل‌های اندازه‌گیری، در اینجا به بررسی وجود یا عدم وجود رابطه علّی میان متغیرهای پژوهش و بررسی تناسب داده‌های مشاهده شده با مدل مفهومی پژوهش، فرضیه‌های پژوهش با استفاده از مدل معادلات ساختاری مورد آزمون قرار گرفتند.



شکل ۲. اندازه‌گیری مدل کلی و نتایج فرضیه‌ها در حالت تخمین استاندارد

Figure 2. General model measurement and hypothesis result in standard estimation mode

تحلیل بوت استراپینگ که مهمترین استفاده از آن در محاسبه مقادیر میانگین، انحراف معیار و مهم‌تر از این دو آماره t است. شکل ۳ خروجی آن را مشاهده می‌کنید. مقادیر موجود در مدل‌های سنجش یعنی ارتباط بین شاخص‌ها با ابعاد و مدل ساختاری یعنی ارتباط بین ابعاد همان مقدار آماره t است.



شکل۳. مدل ترسیم شده همراه با مقادیر t

Figure 3. Model plotted along with t values

برازش مدل عوامل سازمانی

برای برازش مدل عوامل سازمانی شامل فرهنگ سازمانی، خط و مشی سازمانی و پشتیبانی سازمانی به عنوان متغیرهای مستقل، متغیر نگرش به اشتراک‌گذاری دانش به عنوان متغیر وابسته میانجی و متغیر آگاهی از امنیت سایبری به عنوان متغیر وابسته ملاک از شش معیار اصلی شامل مجذور (GOF, SRMR, NFI, Q^2, f^2, R^2) استفاده گردید. نتایج برازش مدل عوامل سازمانی در جدول ۳ نشان داده شده است.

جدول ۳. شاخص‌های برازش مدل عوامل سازمانی

Table 3. Organizational factors model fit indices

متغیرها Variables	اندازه اثر (f^2) Effect size							
	نگرش به اشتراک‌گذاری دانش Information security knowledge sharing attitude	**آگاهی از امنیت سایبری Cyber security awareness**	R^2	Q^2	**مدل اشباع شده Saturated model**	**مدل تخمینی Estimated model**	**مدل اشباع شده Saturated model**	**مدل تخمینی Estimated model**
					SRMR		NFI	
فرهنگ سازمانی Organizational culture	0.003	-						
خط و مشی سازمانی Organizational policy	0.151	-						
پشتیبانی و آموزش سازمانی Organizational support and training	0.343	-						
نگرش به اشتراک گذاری دانش امنیت اطلاعات Information security knowledge sharing attitude	-	0.326	0.672	0.430	0.062	0.063	0.815	0.815
آگاهی از امنیت سایبری Cyber security awareness	-	-	0.246	0.173				

بر اساس جدول ۳، جهت بررسی برازش مدل از شش معیارهای اصلی برازش مدل ساختاری استفاده گردید که در زیر به شرح آن‌ها پرداخته می‌شود:

- R^2 معیاری است که نشان دهنده تأثیری یک متغیر برون زا بر یک متغیر درون زا است که مقدار مورد تأئید برای معیار R^2 سه مقدار ۰/۱۹، ۰/۳۳، و ۰/۶۷ به عنوان مقدار ملاک برای مقادیر ضعیف، متوسط و قوی در نظر گرفته می‌شود. بر اساس جدول فوق، نگرش به اشتراک‌گذاری دانش امنیت اطلاعات با مقدار ۰/۶۷۲ (خیلی قوی) و آگاهی از امنیت سایبری با مقدار ۰/۲۴۶ (متوسط) محاسبه شد. با توجه به مقادیر بدست آمده برازش مدل ساختاری تأئید می‌شود.
- معیار اندازه تأثیر f^2 که رابطه‌ی میان سازه‌های مدل را تعیین می‌کند و مقادیر ۰/۰۲، ۰/۱۵ و ۰/۳۵ به ترتیب نشان از اندازه تأثیر کوچک، متوسط و بزرگ یک سازه بر سازه‌ی دیگر است. بر این اساس، فرهنگ سازمانی بر نگرش به

اشتراک گذاری دانش امنیت اطلاعات فاقد اندازه تأثیر بوده، ولی دو متغیر خط و مشی سازمانی (۰/۱۵۱) و پشتیبانی و آموزش سازمانی (۰/۳۴۳) بر نگرش به اشتراک گذاری دانش امنیت اطلاعات به ترتیب دارای اندازه تأثیر متوسط و قوی می‌باشد.

- معیار Q^2 که در واقع قدرت پیش‌بینی مدل را مشخص می کند در صورتی که این مقدار در مورد یک سازه درون‌زا سه مقدار ۰/۰۲، ۰/۱۵ و ۰/۳۵ حاصل شود به ترتیب نشان دهنده میزان قدرت پیش بینی ضعیف، متوسط و قوی سازه یا سازه‌های برون‌زای مربوط به آن را دارد. در مطالعه حاضر مقدار Q^2 سازه‌ی درون‌زای نگرش به اشتراک گذاری دانش امنیت اطلاعات برابر ۰/۴۳۰ که بیشتر از ۰/۳۵ بوده که نشان از قدرت پیش‌بینی قوی مدل در خصوص این سازه دارد. متغیر آگاهی از امنیت سایبری با مقدار ۰/۱۷۳ که تقریباً در مرز بین متوسط و قوی قرار دارد. این وضعیت حاکی از آن دارد که مدل ساختاری پژوهش مورد تأئید قرار گرفت.

- شاخص NFI یکی دیگر از شاخص های برازش مدل می باشد. اگر مقدار NFI بالای ۰/۷ باشد برازش مدل مناسب است. در پژوهش حاضر این مقدار بالاتر از ۰/۷ یعنی ۰/۰۸ بوده که نشان دهنده برازش مدل مناسب را نشان می دهد.

- برازش کلی با استفاده از معیار GOF، این معیار مربوط به بخش کلی مدل معادلات ساختاری است که توسط تننهاوس و همکاران (۲۰۰۴) ابداء گردید. به منظور بررسی برازش کلی بر اساس معیار GOF از نظر تزلس و همکاران (۲۰۰۹) استفاده گردید. در این دیدگاه در صورتی که مقدار GOF بین ۰/۱ الی ۰/۲۵ ضعیف، بین ۰/۲۵ تا ۰/۳۶ متوسط و اگر از ۰/۳۶ بیشتر باشد قوی می‌باشد. در مطالعه حاضر عدد ۰/۶۱۲ بدست آمد که نشان دهنده برازش کلی مدل در حد قوی می‌باشد.

- معیار بعدی شاخص ریشه میانگین مربعات باقیمانده استاندارد (SRMR) است. این معیار یکی از معیارهای جدیدی است که جایگزین معیار GOF شده است. زیرا GOF نمی‌تواند به طور قابل اعتماد مدل‌های معتبر را از نامعتبر تشخیص دهد. بنابراین استفاده از ریشه میانگین مربعات باقیمانده استاندارد بهتر می‌توان مدل را برازش کند. در واقع، شاخص ریشه میانگین مربعات باقیمانده استاندارد تفاوت بین همبستگی مشاهده شده و ماتریس همبستگی ضمنی مدل توصیف شده است. این شاخص امکان ارزیابی میانگین بزرگی اختلافات بین همبستگی‌های مشاهده شده و مورد انتظار را به عنوان معیار مطلق معیار برازش (مدل) فراهم می کند. مقدار این شاخص کمتر از ۰/۱ در نظر گرفته شده است هرچند برخی از آن را کمتر ۰/۰۸ را پیشنهاد کرده‌اند. در پژوهش حاضر مقدار بدست آمده برابر ۰/۰۶ که نشان دهنده آن است که از تعیین نادرست مدل جلوگیری می کند.

برای بررسی رابطه علّی بین متغیرهای مستقل شامل فرهنگ سازمانی، خط و مشی سازمانی و پشتیبانی و آموزش سازمانی به عنوان متغیرهای مستقل، متغیر نگرش به اشتراک گذاری دانش امنیت اطلاعات به عنوان متغیر وابسته میانجی و متغیر آگاهی از امینت سایبری به عنوان متغیر وابسته ملاک و تأیید کل مدل از روش تحلیل مسیر استفاده شد. نتایج حاصل از خروجی‌های PLS برای پنج فرضیه پژوهش در زیر آمده است.

فرضیه اول تا چهارم پژوهش مبنی بر این بود که فرهنگ سازمانی، خط و مشی سازمانی و پشتیبانی و آموزش سازمانی بر نگرش به اشتراک گذاری دانش امنیت اطلاعات تأثیر مثبت و معناداری دارد. نتایج آزمون این فرضیه در جدول ۴ نشان داده شده است.

جدول ۴. اثر عوامل سازمانی بر نگرش به اشتراک گذاری دانش امنیت اطلاعات

Table 4. Effects of Organizational Factors on Attitudes Toward Information Security Knowledge Sharing

ضریب مسیر Path coefficient	ضریب تأثیر (β)	عدد معناداری (T Statistics)	سطح معناداری (P-values)	نتیجه Decision
خط و مشی سازمانی --> نگرش به اشتراک گذاری دانش امنیت اطلاعات Organizational Policy --> Information security knowledge sharing attitude	0.367	4.064	0.000	تأئید Confirmed
فرهنگ سازمانی --> نگرش به اشتراک‌گذاری دانش امنیت اطلاعات Organizational culture --> Information security knowledge sharing attitude	0.057	0.625	0.532	رد Rejected
نگرش به اشتراک گذاری دانش امنیت اطلاعات --> آگاهی از امنیت اطلاعات Information security knowledge sharing attitude --> Cyber security awareness	0.496	6.020	0.000	تأئید Confirmed
پشتیبانی سازمانی --> نگرش به اشتراک گذاری دانش امنیت اطلاعات Organizational support and training --> Information security knowledge sharing attitude	0.481	6.392	0.000	تأئید Confirmed

همانطوری که در جدول ۴ مشاهده می‌شود، ضریب تأثیر فرهنگ سازمانی بر نگرش به اشتراک گذاری دانش امنیت اطلاعات برابر ۰/۰۵۷ با مقدار آماره t برابر ۰/۶۲۵ شده است که این مقدار از ۱/۹۶ کمتر بوده و با توجه سطح معناداری بدست آمده که بزرگتر از ۰/۰۵ می‌باشد (P>0.5) می‌توان چنین استنباط کرد که فرهنگ سازمانی اثر معناداری بر متغیر نگرش به اشتراک‌گذاری دانش امنیت اطلاعات به عنوان متغیر میانجی ندارد. بنابراین فرضیه اول پژوهش رد شد. اما ضریب تأثیر خط و مشی سازمانی بر نگرش به اشتراک‌گذاری دانش امنیت اطلاعات برابر ۰/۳۶۷ با مقدار آماره t (۴/۰۶۴) شده است که این مقدار از ۱/۹۶ بزرگتر می‌باشد و با توجه سطح معناداری بدست آمده که کوچکتر از ۰/۰۵ می‌باشد (P<0.5) می‌توان چنین استنباط کرد که خط و مشی سازمانی اثر معناداری بر متغیر نگرش به اشتراک‌گذاری دانش امنیت اطلاعات به عنوان متغیر میانجی دارد. بنابراین فرضیه دوم پژوهش تأئید شد. ضریب تأثیر پشتیبانی سازمانی بر نگرش به اشتراک‌گذاری دانش امنیت اطلاعات برابر ۰/۴۸۱ با مقدار آماره t (۶/۳۹۲) شده است که این مقدار از ۱/۹۶ بیشتر بوده و با توجه سطح معناداری بدست آمده که کوچکتر از ۰/۰۵ می‌باشد (P<0.5) می‌توان چنین استنباط کرد که پشتیبانی سازمانی اثر معناداری بر متغیر نگرش به اشتراک‌گذاری دانش امنیت اطلاعات به عنوان متغیر میانجی دارد. بنابراین فرضیه سوم پژوهش تأئید شد. در نهایت ضریب تأثیر نگرش به اشتراک‌گذاری دانش امنیت اطلاعات بر آگاهی از امنیت سایبری برابر۰/۴۹۶ با مقدار آماره t (۶/۰۲۰) شده است که این مقدار از ۱/۹۶ بیشتر بوده و با توجه سطح معناداری بدست آمده که کوچکتر از ۰/۰۵ می‌باشد (P<0.5) می‌توان چنین استنباط کرد که نگرش به اشتراک‌گذاری دانش امنیت اطلاعات اثر معناداری بر آگاهی از امنیت سایبری دارد. بنابراین فرضیه چهارم پژوهش تأئید شد.

فرضیه پنجم پژوهش، فرهنگ سازمانی، خط و مشی سازمانی و پشتیبانی سازمانی با میانجی‌گری نگرش به اشتراک گذاری دانش امنیت اطلاعات بر آگاهی از امنیت سایبری تأثیر مثبت و معناداری دارد. نتایج این آزمون در جدول ۵ نشان داده شده است.

جدول ۵. بررسی اثر کامل متغیرهای پژوهش

Table 5. Assessment of the Total Effects of the Research Variables

ضریب مسیر Path coefficient	اثر کامل Direct effect			اثر غیرمستقیم Indirect effect			نتیجه Decision
	ضریب تأثیر (β)	عدد معناداری (T-statistics)	سطح معناداری (P- values)	ضریب تأثیر (β)	عدد معناداری (T-statistics)	سطح معناداری (P- values)	
خط و مشی سازمانی --> آگاهی از امنیت سایبری Organizational Policy --> Cyber security awareness	0.182	3.444	0.001	0.182	3.444	0.001	تأئید Confirmed
خط و مشی سازمانی --> نگرش به اشتراک گذاری دانش امنیت اطلاعات Organizational Policy --> Information security knowledge sharing attitude	0.367	4.064	0.000	-	-	-	تأئید Confirmed
فرهنگ سازمانی --> آگاهی از امنیت سایبری Organizational culture --> Cyber security awareness	0.028	0.595	0.552	0.028	0.595	0.552	رد Rejected
فرهنگ سازمانی --> نگرش به اشتراک گذاری دانش امنیت اطلاعات Organizational culture --> Information security knowledge sharing attitude	0.057	0.625	0.532	-	-	-	رد Rejected
پشتیبانی سازمانی --> آگاهی از امنیت سایبری Organizational support and training --> Cyber security awareness	0.238	4.436	0.000	0.238	4.436	0.000	تأئید Confirmed
پشتیبانی سازمانی --> نگرش به اشتراک گذاری دانش امنیت اطلاعات Organizational support and training --> Information security knowledge sharing attitude	0.481	6.392	0.000	-	-	-	تأئید Confirmed
نگرش به اشتراک گذاری دانش امنیت اطلاعات --> آگاهی از امنیت سایبری Information security knowledge sharing attitude --> Cyber security awareness	0.496	6.020	0.000	-	-	-	تأئید Confirmed

مطابق جدول ۵، که با استفاده از تحلیل بوت استراپینگ انجام شد، حاکی از آن دارد که سطح معناداری برای اثر کامل و اثر غیر مستقیم متغیرهای خط و مشی سازمانی و پشتیبانی سازمانی بر نگرش به اشتراک گذاری دانش امنیت اطلاعات و آگاهی از امنیت سایبری کمتر از ۰/۰۵ شده است این بدان معنی است که این اثر معنادار بود. اما متغیر فرهنگ سازمانی بر نگرش به اشتراک گذاری دانش امنیت اطلاعات و آگاهی از امینت سایبری بیشتر از ۰/۰۵ بودند و معنادار نبود.

نتیجه‌گیری و بحث

این مطالعه با بررسی بررسی عوامل سازمانی موثر بر قابلیت آگاهی از امنیت سایبری با نقش واسطه‌ای نگرش به اشتراک گذاری دانش امنیت اطلاعات کارکنان شعب بانک‌های کشاورزی شهر کرمانشاه پرداخته است. از نظر کمبود شکاف تحقیقاتی به مجموعه دانش امنیت اطلاعات کمک می‌کند. عواملی همچون فرهنگ سازمانی، خط و مشی سازمانی و پشتیبانی و آموزش سازمانی، نگرش به اشتراک گذاری دانش امنیت اطلاعات و آگاهی از امنیت سایبری مورد بررسی قرار گرفت.

فرضیه اول پژوهش مبنی بر این بود که فرهنگ سازمانی بر نگرش به اشتراک گذاری دانش امنیت اطلاعات تأثیر مثبت و معناداری دارد. نتایج آزمون این فرضیه نشان داد که فرهنگ سازمانی با توجه به آماره های (β=۰/۰۵۷، t= ۰/۵۱۸) نشان داد که اثر معناداری بر متغیر نگرش به اشتراک گذاری دانش امنیت اطلاعات در بین کارکنان نداشت. بنابراین با توجه به سطح معناداری بدست آمده (P>0.5) فرضیه پژوهش رد و فرضیه صفر تأئید شد. این بدان معنی است که در این مطالعه متغیر فرهنگ سازمانی بر نگرش به اشتراک گذاری دانش امنیت اطلاعات اثر معناداری ندارد. نتایج مطالعه حاضر با نتایج برخی از پژوهش‌های پیشین همسو نبود. برای نمونه نتایج پژ.هش (Chen et al., 2015) نشان داد که آگاهی از برنامه‌های آموزش امنیت و آگاهی تأثیرات مهمی بر فرهنگ امنیتی و آگاهی کارکنان از خط‌مشی امنیتی سازمانی دارد و آگاهی از نظارت امنیتی نیز بر فرهنگ امنیتی تأثیر می‌گذارد. نتایج پژوهش شاه بهرامی و همکاران (Shah Bahrami et al., 2017) نشان دادند که عوامل نرم شامل عوامل مدیریتی و فرهنگی نسبت به عوامل سخت شامل عوامل مالی و فنی/ فناورانه درسیستم مدیریت امنیت اطلاعات از اهمیت بیشتری برخوردار بوده و عوامل مدیریتی نسبت به سایر عوامل نرم و همچنین عوامل فنی/ فناورانه نسبت به سایر عوامل سخت دارای بیشترین اهمیت هستند.

نتایج پژوهش (Akter et al., 2022) حاکی از آن داشت که مدیریت (آموزش، فرهنگ و جهت‌گیری استراتژیک) به عنوان ابعاد موضوعی برای مقابله با چالش‌های آگاهی از امنیت سایبری نشان می‌دهد. نتایج پژوهش (Karlsson et al., 2022) نشان دادند که فرهنگ‌های سازمانی با تمرکز داخلی به طور مثبتی با انطباق خط‌مشی امنیت اطلاعات کارکنان مرتبط است. تجزیه و تحلیل نشان می دهد که یک شکل بوروکراتیک از فرهنگ سازمانی برای تقویت انطباق با خط مشی امنیت اطلاعات کارکنان بیشترین سود را دارد. پژوهش(Chen et al., 2015) به این نتیجه دست یافتند که آگاهی برنامه‌های آموزش امنیت و آگاهی تأثیرات قابل‌توجهی بر فرهنگ امنیتی و آگاهی کارکنان از سیاست امنیتی سازمانی دارد و آگاهی از نظارت امنیتی نیز بر فرهنگ امنیتی تأثیر می‌گذارد.

فرضیه دوم پژوهشی مبنی بر این بود که خط و مشی سازمانی بر نگرش به اشتراک گذاری دانش امنیت اطلاعات اثر معناداری دارد. نتایج این پژوهش نشان داد که با توجه به آماره های (β=۰/۳۶۷، t= ۴/۴۵۸) فرهنگ سازمانی اثر معناداری بر متغیر نگرش به اشتراک گذاری دانش امنیت اطلاعات به عنوان متغیر میانجی داشت. بنابراین با توجه به سطح معناداری بدست آمده (P<0.5) فرضیه پژوهش تأئید و فرضیه صفر رد شد. نتایج مطالعه حاضر با نتایج برخی از پژوهش‌های پیشین که به نتایج مشابه این مطالعه دست یافتند، همسو بود. نتایج پژوهش (Shah Bahrami et al., 2017) نشان دادند که عوامل نرم شامل عوامل مدیریتی در سیستم مدیریت امنیت اطلاعات از اهمیت بیشتری برخوردار بود. نتایج پژوهش (Akter et al., 2022) حاکی از آن داشت که مدیریت (آموزش، فرهنگ و جهت‌گیری استراتژیک) به عنوان ابعاد موضوعی برای مقابله با چالش‌های آگاهی از امنیت سایبری نشان می‌دهد. نتایج پژوهش (Singh, Gupta & Ojha, 2014) حاکی از آن داشت که عوامل عملیاتی، استراتژیک و تاکتیکی بر مسائل مدیریت امنیت اطلاعات تأثیر می‌گذارند.

فرضیه سوم پژوهش مبنی بر این بود که پشتیبانی و آموزش سازمانی بر نگرش به اشتراک گذاری دانش امنیت اطلاعات اثر معناداری دارد. نتایج این آزمون نشان داد با توجه به آماره های (β=۰/۴۸۱، t= ۶/۳۰۸) پشتیبانی و آموزش سازمانی اثر معناداری بر متغیر نگرش به اشتراک گذاری دانش امنیت اطلاعات داشت. بنابراین با توجه به سطح معناداری بدست آمده

(P<0.5) فرضیه پژوهش تأئید و فرضیه صفر رد شد. نتایج مطالعه حاضر با نتایج برخی از پژوهش‌های پیشین که به نتایج مشابه این مطالعه دست یافتند، همسو بود. پژوهش (Azar & Mahdavipur, 2022) نشان دادند که عوامل درون سازمانی شامل امن‌سازی تجهیزات، شبکه ها، نرم افزارها، رصد و پایش رخدادهای سایبری و واکنش به موقع به آن ها و ارتقاء دانش سایبری کارکنان و عوامل برون سازمانی شامل تهدیدات سایبری انسان ساز و طبیعی، عوامل موثر بر امنیت سایبری ارتش جمهوری اسلامی ایران را تشکیل می دهند. نتایج پژوهش (Alzahrani & Seth, 2021) نشان دادند که آموزش امنیتی، اشتراک دانش، آموزش امنیتی و دید امنیتی به طور قابل‌توجهی بر عملکرد امنیت اطلاعات تأثیر می‌گذارد. علاوه بر این، این مطالعه تأثیر قابل توجهی از آموزش امنیتی و اشتراک دانش بر اعتماد در سازمان را برجسته می کند. همچنین نتایج پژوهش (Diesch et al., 2020) نشان دادند که آموزش امنیتی، اشتراک دانش، آموزش امنیتی و دید امنیتی به طور قابل‌توجهی بر عملکرد امنیت اطلاعات تأثیر می‌گذارد. همچنین (Parsons et al. 2014) دریافتند که کمپین های آموزشی و آموزشی تأثیر مثبتی بر دانش کارکنان از خط مشی ها و رویه ها داشته است.

فرضیه چهارم پژوهش مبنی بر این بود که فرهنگ سازمانی، خط و مشی سازمانی و پشتیبانی و آموزش سازمانی با میانجی گری نگرش به اشتراک گذاری دانش امنیت اطلاعات بر آگاهی از امنیت سایبری تأثیر مثبت و معناداری دارد. نتایج حاکی از آن داشت که سطح معناداری برای اثر کامل و اثر غیرمستقیم متغیرهای خط و مشی سازمانی و پشتیبانی و آموزش سازمانی بر نگرش به اشتراک گذاری دانش امنیت اطلاعات و آگاهی از امنیت سایبری کمتر از ۰/۰۵ شد (P<0.5). این بدان معنی است که این اثر معنادار بود. اما متغیر فرهنگ سازمانی بر نگرش به اشتراک گذاری دانش امنیت اطلاعات و آگاهی از امینت سایبری بیشتر از ۰/۰۵ بود و این متغیر معنادار نشد(P>0.5).

در پاسخ به این سوال که آیا مدل عوامل سازمانی از برازش مطلوبی برخوردار می‌باشد یا خیر؟ به منظور بررسی این سوال از شش معیار اصلی شامل (GOF, SRMR, NFI, Q^2, f^2, R^2) استفاده گردید. نتایج R^2 نشان داد که متغیر نگرش به اشتراک گذاری دانش امنیت اطلاعات با مقدار ۰/۶۷۲ (خیلی قوی) و آگاهی ار امنیت سایبری با مقدار ۰/۲۴۶ (متوسط) محاسبه شد که نشان دهنده برازش مدل ساختاری می باشد. نتایج معیار اندازه تأثیر f^2 فرهنگ سازمانی بر نگرش به اشتراک‌گذاری دانش امنیت اطلاعات فاقد اندازه تأثیر بوده، ولی دو متغیر خط و مشی سازمانی (۰/۱۵۱) و پشتیبانی سازمانی (۰/۳۴۳) بر نگرش به اشتراک گذاری دانش امنیت اطلاعات به ترتیب دارای اندازه تأثیر متوسط و قوی می‌باشد. معیار Q^2 نشان داد که مقدار Q^2 سازه‌ی درون‌زای نگرش به اشتراک گذاری دانش امنیت اطلاعات برابر ۰/۴۳۰ که بیشتر از ۰/۳۵ می‌باشد که نشان از قدرت پیش بینی قوی مدل در خصوص این سازه دارد. متغیر آگاهی از امنیت سایبری با مقدار ۰/۱۷۳ که تقریباً در مرز بین متوسط و قوی قرار دارد. شاخص NFI بالاتر از ۰/۷ یعنی ۰/۰۸ بوده که نشان دهنده برازش مدل مناسب را نشان می دهد. نتایج معیار ریشه میانگین مربعات باقیمانده استاندارد (SRMR) نشان داد که مقدار بدست آمده برابر ۰/۰۶ که نشان دهنده آن است که از تعیین نادرست مدل جلوگیری می کند. در نهایت برازش کلی با استفاده از معیار GOF، ۰/۶۱۲ بود که نشان دهنده برازش کلی مدل در حد قوی می باشد. به طور کلی نتایج برازش هر دو مدل نشان داد که از برازش مناسب برخوردار بودند. بر اساس نتایج این مطالعه، پیشنهادهای زیر توصیه می شود:

- پیشنهاد می‌شود که بانک، اقدام به تدوین خط و مشی و یا تدیون سیاست‌های امنیت اطلاعات و تهدیدات سایبری اقدام نماید. این سیاست راهبردهای امنیت اطلاعات در کارکنان هدایت و در تقویت آگاهی کارکنان نقش موثری خواهد داشت.
- پیشنهاد می‌شود بانک نسبت به اقدامات امنیتی و حفظ حریم خصوصی بانک و کارکنان طراحی کنند. این اقدامتی امنیتی علاوه بر افزایش آگاهی از تهدیدات سایبری می شود موجب کاهش خطاها و اشتباهات کارکنان دز استفاده از سیستم های فناوری اطلاعات در بانک خواهد شد.

- پیشنهاد می‌شود خدمات مشاوره‌ای به صورت شبانه روزی در بانک استان فعال تا در صورت هر گونه مشکلی به برطف کردن آن مشلک پرداخته شود.

- پیشنهاد می‌شود بانک نسبت به آموزش مهارت‌های جدید در قالب مهارت‌های امنیتی بپردازند که این نوع آموزش می‌تواند منجر به پیشگیری از رفتار پرخطر فضای اینترنت یا فضای مجازی شود.

در پایان پیشنهاد می‌شود که سازمان‌ها باید قابلیت‌های امنیت اطلاعات خود را افزایش دهند تا به چالش‌ها و خطرات جدید پاسخ خلاقانه بدهند تا بقای خود را در این محیط بسیار رقابتی تضمین کنند.

محدودیت‌های پژوهش

هر پژوهشی دارای محدودیت‌های خاص خود می‌باشد که از اختیار پژوهشگر خارج بوده است. این مطالعه بر روی کارکنان بانک کشاورزی شهرستان کرمانشاه انجام شده است. بنابراین از تعیمم دادن به سایر جوامع دیگر بایستی با احتیاط انجام شود. همچنین ابزار گردآوری داده‌ها در یک مقطع زمانی خاص انجام شده است این بدان معنی است که اعتبار آن در دوره زمانی کوتاهی صورت گرفته است. این ممکن است در گذشت زمان بر متغیرهای مورد بررسی در این مطالعه اثر داشته باشد و سبب تغییر نتایج شود.

تعارض منافع

هیچ گونه تعارض منافعی وجود ندارد.

قدردانی و تشکر

از کلیه افرادی که در این پژوهش مشارکت داشتند، تقدیر و تشکر می‌گردد.

References

Ahlan, A. R. & Lubis, M. & Lubis, A. (2015). Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science*. 72. 361-373. https://doi.org/10.1016/j.procs.2015.12.151

Al-Kurdi, O., El-Haddadeh, R., & Eldabi, T. (2018). Knowledge sharing in higher education institutions: a systematic review. *Journal of Enterprise Information Management, 31(2), 226–246.* https://doi.org/10.1108/JEIM-09-2017-0129

Akter, S. et al. (2022). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. *Annals of Operations Research*, 2:1-26. https://doi.org/10.1007/s10479-022-04844-8

Akturan, A. and Çekmecelioglu, H.G. (2016). The effects of knowledge sharing and organizational citizenship behaviors on creative behaviors in educational institutions. *Procedia – Social and Behavioral Sciences*, 235, 342-350, https://doi.org/10.1016/j.sbspro.2016.11.042

Alhassan, M.M. & Adjei-Quaye, A. (2017). Information security in an organization. *International Journal of Computer (IJC)*, 24(1), 100-116.

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 49, 567-575. https://doi.org/10.1016/j.chb.2015.03.054

Allen, J.H. et al. (2015). *Structuring the chief information security officer organization*. Carnegie Mellon University.

Alzahrani, L. & Seth, K.P. (2021). The Impact of organizational practices on the information security management performance. *Information*, 12 (398), 1-16. https:// doi.org/10.3390/info12100398

Azar, D. and Mahdavipur, M. (2022). I.R.I Army cybersecurity effective factors. (Case study: I.R.I Army general staff). *Military Science and Tactics*, 18 (60), 103-123. [In Persian]

Cabrera, A. & Cabrera, E.F. (2002). Knowledge-sharing dilemmas. *Organization Studies*, 23(5), 687-710. https://doi.org/10.1177/01708406022350

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2015). Institutional pressures in security management: direct and indirect influences on organizational investment in information security control resources. *Information & Management*, 52(4), 385-400. http://dx.doi.org/10.1016/j.im.20 14.12.004.

Chen, Y., Ramamurthy, K.(Ram) & Wen, K-W. (2013). Organization's information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems* (29:3), 163-195. https://doi.org/10.2753/MIS0742-1222290305

Chen, Y., Ramamurthy, K.(Ram). & Wen, K.-W. (2015). Impacts of Comprehensive Information Security Programs on Information Security Culture. *Journal of Computer Information Systems,* 55(3), 11–19. https://doi.org/10.1080/08874417.2015.11645767

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not. *Information & Computer Security*, 24(2), 139 – 151. https://doi.org/10.1108/ICS-12-2015-0048

Da Veiga, A. & Eloff, J.H.P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29 (2), 196-207. https://doi.org/10.1016/j.cose.2009.09.002

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

Feledi, D., Fenz, S. & Lechner, L. (2013). Toward web-based information security knowledge sharing. *Information Security Technical Report*, 17(4), 199-209. https://doi.org/10.1016/j.istr.2013.03.004

Flores, W.R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 43, 90-110. https://doi.org/10.1016/j.cose.2014.03.004

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18 (1), 39–50. https://doi.org/10.2307/3151312

Gcaza, N., von Solms, R., Grobler, M.M. & van Vuuren, J.J. (2017). A general morphological analysis: delineating a cyber-security culture. *Information and Computer Security*, 25(3), 259-278. https://doi.org/10.1108/ICS-12-2015-0046

Hellriegel, D., Slocum, J.W. Jr & Woodman, R.W. (1998). *Organizational behavior*. 8th ed. South-Western College Publishing, PA.

Islam, M.S., Kunifuji, S., Hayama, T. & Miura, M. (2013). Knowledge sharing practices among doctoral students in JAIST to enhance research skills. *Knowledge Management and ELearning*, 5(2), 170-185. https://www.kmel-journal.org/ojs/index.php/online-publication/article/view/202

Karlsson, M., Karlsson, F., Åström, J. & Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. *Information and Computer Security*, 30(3), 382-401. https://doi.org/10.1108/ICS-06-2021-0073.

Khan, N.F., Ikram, N., Saleem, S. & Zafar, S. (2023). Cyber-security and risky behaviors in a developing country context: a Pakistani perspective. *Security Journal*, 36, 373–405 (2023). https://doi.org/10.1057/s41284-022-00343-4.

Kiashmeshki , M.A. & Daneshvar, A. (2022). Use of Structural Equation Modeling for Agent-based Modeling and Simulation in the Analysis of Information Security Knowledge Sharing. Scientific Journal Of Organizational knowledge Management, 5 (18), 151-199. [In Persian]

Kim, H.L., Choi, H.S. & Han, J. (2019). Leader power and employees' information security policy compliance. *Security Journal*, 32, 391–409. https://doi.org/ 10.10 57/s41284-019-00168-8.

Lawshe, C. H. (1975). A quantitative approach to content validity. *Personnel Psychology, 28*(4), 563–575. https://doi.org/10.1111/j.1744-6570.1975.tb01393.x

Ma, X. (2022). Is professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing & Management*, 59(1), 102744, 1-14. doi.org/10.1016/j.ipm.2021.102744

Mejias RJ. (2012). An integrative model of information security awareness for assessing information systems security risk. InSystem Science (HICSS), 2012 45th Hawaii International Conference on 2012 Jan 4 (pp. 3258-3267). IEEE. DOI: 10.1109/HICSS.2012.104

Mirzaei Ahranjani, H. (1998). In search of a theoretical plan to recognize and analyze the factors affecting work conscience and social discipline, the collection of articles of the second meeting of examining the practical ways of governance of work conscience and social discipline, Islamic Azad University, Qazvin branch. [In Persian]

Narain Singh, A., Gupta, M.P. & Ojha, A. (2014). Identifying factors of organizational information security management. *Journal of Enterprise Information Management*, 27(5), 644-667. https://doi.org/10.1108/JEIM-07-2013-0052.

Nielsen, C. & Cappelen, K. (2014). Exploring the mechanisms of knowledge transfer in universityindustry collaborations: a study of companies, students and researchers. *Higher Education Quarterly*, 68(4), 375-393, doi: 10.1111/hequ.12035.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Compuer. Secur*ity, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Obitade, P.O. (2019). *Big data analytics: a link between knowledge management capabilities and superior cyber protection*. *Journal of Big Data*, 6(71). https://doi.org/10.1186/s40537-019-0229-9

Safa, N.S. & Ismail, M.A. (2013). A customer loyalty formation model in electronic commerce. Economic Modelling,35(0):559e64. https://doi.org/10.1016/j.econmod.2013.08.011

Safa, N.S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, 57(442e451), 442-451. doi.org/ 10.1016/j.chb.2015.12.037

Safa, N.S., Von Solms, R. & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 1–13. https://doi.org/10.1016/j.cose.2015.10.006

Schlienger, T. & Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. 14th International Workshop on Database and Expert Systems Applications (DEXA'03), Prague, Czech Republic, 2003. DOI:10.1109/DEXA.2003.1232055

Shah Bahrami, A., Rafizadeh Kasani, R. & Poriosofi Dargah, H. (2017). Identifying and prioritizing parameters affecting the information security management system (case study: social security branches of Gilan province). *Journal of Information and Communication Technology*, 10 (35-36), 57-74. [In Persian]

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: predicting initial adoption of information security behavior. *Computers & Security*, 49(0), 177e191. https://doi.org/10.1016/j.cose.2015.01.002

Schlienger, T. & Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. 14th International Workshop on Database and Expert Systems Applications (DEXA'03), Prague, Czech Repu.

Straub, D., Boudreau, M-C & Gefen, D. (2004). Validation guidelines for is positivist research. *Communications of the AIS,* (13), 380-426. https://doi.org/10.17705/1CAIS.01324

Taghipoor, R. & Esmaeili, A. (2019). Designing a conceptual model of the cyber defense model of the Islamic Republic of Iran. *Journal of National Security*, 8 (31), 181-202. [In Persian]

Tamjidyamcholo, A., Bin Baba, M.S., Tamjid, H., & Gholipour, R. (2013). Information security – Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers & Education, 68, 223–232.* doi: 10.1016/j.compedu.2013.05.010.

Tang, M., Li, M. & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, 1-8. https://doi.org/10.1007/s10799-015-0252-2

Van Niekerk, J.F. & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security,* 29(4), 476-486. https://doi.org/10.1016/j.cose.2009.10.005

Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Waltz, CF., & Bausell, RB. (1981). *Nursing Research: Design, Statistics, and Computer Analysis*. Philadelphia: W.B. Saunders Co; P. 45.

Wang, S. & Noe, R.A. (2010). Knowledge sharing: a review and directions for future research. *Human Resource Management Review*, 20(2), 115-131. https://doi.org/10.1016/j.hrmr.2009.10.001

Warner, M. (2012). Cybersecurity: A Pre-history. *Intelligence and national security*, 27 (5), 781-799. DOI: 10.1080/02684527.2012.708530

Wilson, M. & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program. NIST Special Publication 800-50, National Institute of Standards and Technology, U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-50

Wu, I.-L., Chuang, C.-H., & Hsu, C.-H. (2014). *Information sharing and collaborative behaviors in enabling supply chain performance: A social exchange perspective*. *International Journal of Production Economics*, 148, 122-132. doi.org/10.1016/j.ijpe.2013.09.016

Yesil, S., Koska, A. & Büyükbese, T. (2013). Knowledge sharing process, innovation capability and innovation performance: an empirical study. *Procedia –Social and Behavioral Sciences*, 75, 217-225, doi: 10.1016/j.sbspro. 2013.04.025.

Yi, J. (2009). A measure of knowledge sharing behavior: scale development and validation. *Knowledge Management Research & Practice*, 7(1), 65-81. https://doi.org/10.1057/kmrp.2008.36