Investigating the Effect of Moral Disengagement and Organizational Culture on Behaviors Related to Information Security Awareness; Case Study Saderat and Mellat Banks

Tooraj Ghahremani*
Master of Science in Information Technology Management;
Payame Noor University; Tehran, Iran;
Email: Toorajghahremani@gmail.com

Farhad Farnia
PhD Candidate in Strategic Management in Cyber Space;
Supreme National Defense University; Tehran, Iran;
Email: Fa.Farnia99@sndu.ac.ir

Received: 22, Oct. 2022 **Accepted: 11, Oct. 2023**

Abstract: When it comes to information security (IS), human behavior is a factor that should not be underestimated. Information Security Awareness (ISA) programs are in place as a preventative measure, but data security breaches still exist, and banks hold valuable personal and financial information that makes them a target for cybercriminals. Based on this, the aim of the present study is to investigate the effect of moral disengagement and organizational culture on behaviors related to information security awareness, taking into account the mediating role of cognitive- effective variables of ISA (knowledge and attitude) and security culture of employees of Saderat and Mellat banks. The current research is applied in terms of its purpose, and in terms of data collection it is descriptive and correlational and is based on the structural equation model. The statistical population of the research was the employees of Mellat and Saderat Bank branches in Tehran. In this regard, the sample size was estimated to be 430 people. In this study, descriptive analysis method with SPSS software and partial least squares (PLS) approach with Smart PLS software were used for data analysis. Because the use of the partial least squares approach as a method of evaluating relationships between variables related to human behavior in the field of information security has been the most common approach in quantitative studies. The findings of the research confirmed the relationships of

* Corresponding Author

Iranian Journal of Information Processing and Management

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Vol. 39 | No. 2 | pp. 453-476
Winter 2024
https://doi.org/10.22034/jipm.2023.709000

the model and the path analysis results showed the influence of the variable “moral disengagement” on the variables of “information security awareness behaviors” (first hypothesis), “information security awareness knowledge” (second hypothesis) and “information security awareness attitude” (third hypothesis) is significantly negative. Also, the effect of the variable “information security awareness knowledge” on “information security awareness behaviors” (fourth hypothesis), the effect of the “information security awareness attitude” variable on “information security awareness behaviors” (fifth hypothesis), the effect of the “organizational culture” variable” on the variables of “information security awareness behaviors” and “organizational security culture” (sixth and seventh hypotheses) and the effect of the “organizational security culture” variable on “information security awareness behaviors” (eighth hypothesis) is positive and significant.

Keywords: Moral Disengagement, Organizational Culture, Security Culture, Information Security Awareness Behaviors, Cognitive-Emotional Variables, Employees of Banks, Bank Mellat, Bank Saderat

بررسی تأثیر بی‌تفاوتی اخلاقی و فرهنگ سازمانی بر رفتارهای مرتبط با آگاهی از امنیت اطلاعات؛

مورد مطالعه بانک‌های صادرات و ملت

تورج قهرمانی
کارشناسی ارشد مدیریت فناوری اطلاعات؛ دانشگاه پیام نور؛ تهران، ایران؛
پدیدآور رابط Toorajghahremani@gmail.com

فرهاد فرنیا
دانشجوی دکتری مدیریت راهبردی فضای سایبر؛ دانشگاه عالی دفاع ملی؛ تهران، ایران؛
Fa.Farnia99@sndu.ac.ir

پژوهش‌نامهٔ پردازش و مدیریت اطلاعات

دریافت: ۱۴۰۱/۰۷/۳۰ **پذیرش:** ۱۴۰۲/۰۷/۱۹ مقاله برای اصلاح به مدت ۷۵ روز نزد پدیدآوران بوده است.

نشریهٔ علمی | رتبهٔ بین‌المللی
پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)
شاپا (چاپی) ۸۲۲۳-۲۲۵۱
شاپا (الکترونیکی) ۸۲۳۱-۲۲۵۱
نمایه در LISTA، ISC، و SCOPUS
jipm.irandoc.ac.ir
دورهٔ ۳۹ | شمارهٔ ۲ | ص‌ص ۴۵۳-۴۷۶
زمستان ۱۴۰۲
https://doi.org/10.22034/jipm.2023.709000

چکیده: وقتی صحبت از امنیت اطلاعات می‌شود، رفتار انسان عاملی است که نباید آن را دست کم گرفت. برنامه‌های آگاهی از امنیت اطلاعات به‌عنوان یک اقدام پیشگیرانه وضع شده‌اند؛ اما موارد نقض امنیت اطلاعات همچنان وجود دارد و بانک‌ها دارای اطلاعات شخصی و مالی ارزشمندی هستند که آن‌ها را به هدف مجرمان سایبری تبدیل می‌کند. بر این اساس، هدف پژوهش حاضر بررسی تأثیر بی‌تفاوتی اخلاقی و فرهنگ سازمانی بر رفتارهای مرتبط با آگاهی از امنیت اطلاعات با در نظر گرفتن نقش میانجی متغیرهای شناختی احساسی (دانش و نگرش) و فرهنگ امنیتی کارکنان بانک‌های صادرات و ملت است. پژوهش حاضر از لحاظ هدف، کاربردی محسوب می‌شود و از نظر نحوه گردآوری داده‌ها، توصیفی و از نوع همبستگی بوده و بر مدل معادله‌های ساختاری مبتنی است. جامعه آماری پژوهش، کارکنان شعب بانک‌های ملت و صادرات در شهر تهران بودند. در این راستا حجم نمونه ۴۳۰ نفر برآورد گردید. در این مطالعه برای تحلیل داده‌ها از روش تحلیل توصیفی با نرم‌افزار SPSS و رویکرد حداقل مربعات جزئی (PLS) با نرم‌افزار Smart PLS استفاده شده است؛ چرا که استفاده از رویکرد حداقل مربعات جزئی به‌عنوان روش ارزیابی روابط بین متغیرهای مرتبط با رفتار انسان در حوزه امنیت اطلاعات، متداول‌ترین

رویکرد در مطالعات کمی بوده است. یافته‌های پژوهش، روابط مدل را تأیید نمود و نتیجه تحلیل مسیر نشان داد که تأثیرگذاری متغیر «بی‌تفاوتی اخلاقی» بر متغیرهای «رفتارهای آگاهی از امنیت اطلاعات» (فرضیه اول)، «دانش آگاهی از امنیت اطلاعات» (فرضیه دوم) و «نگرش آگاهی از امنیت اطلاعات» (فرضیه سوم) منفی و معنادار است. همچنین تأثیر متغیر «دانش آگاهی از امنیت اطلاعات» بر «رفتارهای آگاهی از امنیت اطلاعات» (فرضیه چهارم)، تأثیر متغیر «نگرش آگاهی از امنیت اطلاعات» بر «رفتارهای آگاهی از امنیت اطلاعات» (فرضیه پنجم)، تأثیر متغیر «فرهنگ سازمانی» بر متغیرهای «رفتارهای آگاهی از امنیت اطلاعات» و «فرهنگ امنیتی سازمان» (فرضیه‌های ششم و هفتم) و تأثیر متغیر «فرهنگ امنیتی سازمان» بر «رفتارهای آگاهی از امنیت اطلاعات» (فرضیه هشتم) مثبت و معنادار است.

کلیدواژه‌ها: بی‌تفاوتی اخلاقی، فرهنگ سازمانی، فرهنگ امنیتی، رفتارهای آگاهی از امنیت اطلاعات، متغیرهای شناختی احساسی، کارکنان بانک‌ها، بانک ملت، بانک صادرات

۱. مقدمه

بیش از یک دهه است که بانک‌ها به‌شدت نیازمند بهبود امنیت اطلاعات هستند (Baskerville, Spagnoletti & Kim 2014). بانک‌ها در یک محیط جهانی پیچیده، تحت نظارت، و به‌سرعت در حال پیشرفت حضور دارند؛ به شکلی که انجام عملیات در این محیط مستلزم فناوری‌هایی است که نوظهور بوده و به‌طور مداوم در حال تغییرند (Goldstein, Chernobai & Benaroch 2011). در عین حال، این مؤسسات مالی اهدافِ اصلی برای وقوع جرم و کلاه‌برداری محسوب می‌شوند (Norton & Walker 2014). در نتیجه، به‌طور فزاینده‌ای توسط خطرات امنیت اطلاعات مرتبط با داده و عملیات، که منجر به افزایش سطح نقض امنیت اطلاعات در سراسر جهان می‌شوند، تهدید می‌شوند (Pricewaterhouse Coopers 2014). در این راستا گزارش‌های رسانه‌ایِ مستمری در مورد نقض امنیت اطلاعات در بانک‌ها در سطح جهانی وجود دارد. برای نمونه، به‌تازگی اطلاعات شخصیِ ۱۵ میلیون کارتِ بانکی در ایران، طی بزرگ‌ترین رویداد امنیت بانکداری در تاریخ این کشور در یکی از شبکه‌های اجتماعی منتشر شد (Fassihi & Bergman 2019). همچنین شرکت بیمه سپرده فدرال[1] در مورد پنج حادثه مهم بانکی که هر کدام شامل بیش از ۱۰۰۰۰ رکوردِ داده بود، به کنگره ایالات متحده گزارش داده است. این شرکت بیمه پیش‌تر نیز در ارتباط با حادثه‌ای که توسط یک کارمندِ در حال جدا شدن از بانک که به‌طور

1. The Federal Deposit Insurance Corporation (FDIC)

تصادفی داده‌های حدوداً ۴۴۰۰۰ مشتری FDIC را نقض کرده بود، گزارشی را ارائه کرده بود (Davidson 2016). از این‌رو، مدیریت حرفه‌ای امنیت اطلاعات برای مقابله با خطرات این حوزه بسیار مهم است (Hsu, Backhouse & Silva 2014).

چندین راه‌کار فناورانه برای افزایش امنیت اطلاعات وجود دارد (برای نمونه، دیوارهای آتش و نرم‌افزار ضدویروس)؛ اما گزارش‌ها نشان می‌دهند که رفتار انسان عامل آسیب‌پذیری است که نباید نادیده گرفته شود (Ernst & Young Global Limited 2019; Nctv. 2019). کاربران همواره با رفتارهای ارادی و یا غیرارادی باعث بروز حوادث امنیت اطلاعات می‌شوند؛ مانند مدیریت سهل‌انگارانهٔ اطلاعات، گشت‌وگذار در صفحات وبِ ناامن و استفاده بی‌رویه از دستگاه‌های تلفن همراه یا داده‌های ناامن (Siponen & Vance 2010; Stanton et al. 2005). رفتار مخاطره‌آمیز می‌تواند فرصت‌های بیشتری را در اختیار همکاران داخلیِ مخرب یا عاملانِ خارجی برای آسیب رساندن به بانک قرار دهد (Guo 2013). رفتارهای مُخرب و کلاه‌برداری، مانند سرقت داده‌های محرمانه، با ترکیبی از رفتارهای پرخطر کارکنان امکان‌پذیر است (Warkentin & Willison 2009). در طول دهه گذشته، بانک‌ها شروع به اجرای کنترل‌های پیشگیرانه مانند خط‌مشی‌های امنیت اطلاعات[1] کرده‌اند، که یک استاندارد الزام‌آور در مورد رفتارهای امنیت اطلاعات را در بین تمام کاربران ایجاد می‌کند تا حوادث زیان‌بار مربوط به امنیت اطلاعات را کاهش دهد(Höne & Eloff 2002). خط‌مشی‌های امنیت اطلاعات الزامات امنیتی خاصی را مشخص می‌کنند، اما به تنهایی مؤثر نیستند (Warkentin & Willison 2009). از این‌رو، بانک‌ها برنامه‌هایی را برای افزایش آگاهی از امنیت اطلاعات[2] اجرا می‌کنند (Kajzer et al. 2014).

آگاهی از امنیت اطلاعات به‌عنوان حالتی تعریف می‌شود که «کارمندان سازمان از مأموریت امنیتیِ خود آگاه هستند» (Siponen 2000, 31). آگاهی از امنیت اطلاعات یک چالش بلندمدت است (Goodhue & Straub 1991) و نوآوری‌های فناورانه باعث می‌شوند که کاربران در مورد تهدیدهای جدیدِ امنیت اطلاعات با مشکل مواجه شوند (Baskerville, Spagnoletti & Kim 2014). برنامه‌های ISA ساختاریافته، توسط سازمان‌ها جهت آموزش کارکنان در زمینه خطرات امنیت اطلاعات و نحوه رفتار آن‌ها جهت مطابقت با خط‌مشی‌های امنیت اطلاعات مورد بهره‌برداری قرار می‌گیرند (Johnson 2006). بر

1. information security policy (ISP) 2. information security awareness (ISA)

این اساس، برنامه‌های ISA شامل مداخلات آگاهی‌بخشِ برنامه‌ریزی‌شده‌ای هستند که هدف آن‌ها انتقال مداوم اطلاعات امنیتی به مخاطبان هدف است (Siponen 2000). این مداخلات ممکن است شامل پیام‌های اینترانت، پوسترها، لیوان چاپ‌شده یا آموزش‌های الکترونیک برای افزایش آگاهی کارمندان از امنیت اطلاعات و کاهش رفتار مخاطره‌آمیزِ ارادی و غیرارادی آن‌ها باشد.

در این راستا در طی دهه گذشته، در خارج از ایران و در زمینه پژوهش‌های مربوط به نقش عوامل انسانی در آگاهیِ کارکنان از امنیت اطلاعات (ISA)، رشد چشمگیری وجود داشته است؛ برای نمونه: Hadlington et al. (2019); McCormac et al. (2018). بیشتر این پژوهش‌ها بر تفاوت‌های فردیِ مربوط به جنسیت، سن و ویژگی‌های شخصیتی مانند توافق‌پذیری و وظیفه‌شناسی متمرکز بوده‌اند (McCormac et al. 2017). با این حال، پژوهش‌های جدیدتر بررسی کرده‌اند که چگونه آگاهی از امنیت اطلاعات با تفاوت‌های فردیِ مبتنی بر شغل از جمله منبع کنترل کاری[1]، هویت کاری[2] و مشارکت در فعالیت‌های اینترنتیِ در محل کار[3] مرتبط‌اند (Hadlington et al. 2019; Hadlington & Parsons 2017). حتی اگر پژوهش‌ها در این زمینه همچنان در حال رشد باشد، درک فعلی ما از تأثیر تفاوت‌های فردی بر ISA هنوز بسیار ناچیز است. برای نمونه، پژوهش‌های محدودی در زمینه بررسی تأثیر متقابل بین التزام به ISA و تمایل به بی‌تفاوتی اخلاقی (یک عامل اصلی در زمینه عضویت سازمانی ناکارآمد یا غیرمؤثر) انجام شده است. بی‌تفاوتی اخلاقی[4] عبارت است از «یک مکانیسم بالقوه مقابله‌ای برای حل‌وفصل فشارهای ناشی از الزامات امنیتی در محل کار» (D'Arcy, J., T. Herath, & M. K. Shoss 2014).

از طرفی، رفتار انسان تا حد زیادی توسط فرهنگ تحت تأثیر قرار گرفته و فرهنگ بر تعاملات در محیط‌های اجتماعی و کاری روزمره اثرگذار است (Cronk 2017). بنابراین، هنگام تلاش برای درک و شکل دادن به رفتار انسان، توجهِ صِرف به فرد، مشکل‌ساز خواهد بود. همچنین در نظر گرفتن گروه، سیستم‌های اجتماعی و اقتصادیِ گسترده‌تر و تعاملات آن‌ها بسیار مهم است (Tessem & Skaaraas 2005). این موضوع برای امنیت اطلاعات مهم است، زیرا افراد نه‌تنها در ایجاد خطرات، بلکه در جلوگیری از نقضِ امنیت نیز نقش به‌سزایی دارند (Wiley, McCormac & Calic 2020).

1. work locus of control 2. work identity 3. cyber loafing activities 4. morally disengage

به‌منظور درک بیشتر نقش افراد در امنیت اطلاعات، هدف اصلی این مطالعه بررسی تأثیر بی‌تفاوتی اخلاقی و فرهنگ سازمانی بر رفتارهای مرتبط با آگاهی از امنیت اطلاعات با در نظر گرفتن نقش میانجی جنبه‌های شناختی-احساسیِ ISA (دانش و نگرش) و فرهنگ امنیتی سازمان است. در این راستا و بر اساس جست‌وجوی پژوهشگرانِ پژوهشِ حاضر، تاکنون این سازه‌ها به‌صورت تجربی و به شکل ترکیبی و در قالب یک مدل مفهومی بررسی نشده‌اند. از طرفی، این پژوهش بر توسعه و بسط مدل‌های ارائه‌شده در مقاله‌های Hadlington, Binder & Stanulewicz (2021); Wiley, McCormac & Calic (2020) تمرکز دارد. بر همین اساس، پژوهش حاضر از لحاظ مفهومی نیز دارای نوآوری است. همچنین با توجه به اینکه عوامل مؤثر بر آگاهی از امنیت اطلاعات در مقالات مزبور در جامعه‌ای متشکل از کارکنان صنایع مختلف که عمدتاً به‌صورت نیمه‌وقت شاغل بوده‌اند، مورد مطالعه قرار گرفته، با در نظر گرفتن این جامعه، کارمندان بانک به‌عنوان یک هدف اصلی برای هکرهایی که قصد دسترسی به مناطقِ حساسِ سیستم‌های بانکی از طریق حملات سایبری را دارند، تا حدودی نادیده گرفته شده‌اند. این مسئله در حوزه فناوری اطلاعات در صنعت بانکداری حیاتی محسوب می‌شود. از این‌رو، یکی از اهداف این پژوهش پُرکردن این شکاف تحقیقاتی است. در ادامه، ابتدا مدل تحقیق و فرضیه‌ها ارائه شده و سپس، با بیان روش پژوهش، داده‌های تحقیق، ابزار گردآوری آن‌ها و جامعه آماری مطرح می‌شوند. پس از آن به تجزیه‌وتحلیل داده‌ها پرداخته و سرانجام، نتایج و پیشنهادات ارائه می‌شود.

۲. پیشینه پژوهش

پژوهش در زمینه آگاهی از امنیت اطلاعات، بی‌تفاوتی اخلاقی و فرهنگ سازمانی به‌طور قابل ملاحظه‌ای در دهه گذشته افزایش یافته است. در این راستا پژوهشگران با مطالعه پژوهش‌های پیشین، مقالاتی را که با محوریت این مفاهیم بودند، مورد بررسی قرار داده‌اند. در ادامه، به برخی از پژوهش‌های مرتبط اشاره شده است.

در پژوهش «هندلینگتون، بایندر و استانلوویچ» به بررسی تأثیر بی‌تفاوتی اخلاقی بر رفتارهای آگاهی از امنیت اطلاعات پرداخته شده است. جامعه آماری این پژوهش ۷۱۸ نفر از افراد ۱۸ تا ۶۴ سال بودند که از بستر نرم‌افزاریِ اشتراکی Qualtrics استفاده می‌کردند. نتایج پژوهش نشان داد که گرایش به بی‌تفاوتی اخلاقی تأثیر منفی و معنادار بر ISA، نگرش و دانش داشته و دانش ISA و نگرش ISA بخشی از یک مکانیسم واسطه‌ای

هستند که زیربنای رابطه بین بی‌تفاوتی اخلاقی و ISA محسوب می‌شوند (Hadlington, Binder & Stanulewicz 2021). همچنین در پژوهش «وایلی، مک‌کورمیک و کالیک» به بررسی تأثیر فرهنگ سازمانی بر آگاهی از امنیت اطلاعات با نقش میانجی فرهنگ امنیتی پرداخته شده است. در این پژوهش در کل ۵۰۸ استرالیایی (۳۰۰ زن، ۲۰۷ مرد، یک جنس مشخص نشده) شاغل پرسشنامه (آنلاین) را تکمیل کردند. شرکت‌کنندگان عمدتاً کارکنان موقت (غیررسمی) یا قراردادی (n = ۳۰۳)، و در مقایسه با کارکنان تمام‌وقت (n = ۱۳۸) یا کارکنان نیمه‌وقت (n = ۶۷) و به‌طور مساوی دارای مشاغل مدیریتی (n = ۲۵۵) و غیرمدیریتی (n = ۲۵۳) بودند. یافته‌های پژوهش نشان داد که فرهنگ سازمانی بر آگاهی از امنیت اطلاعات تأثیرگذار بوده و فرهنگ امنیتی در این رابطه نقش میانجی را ایفا می‌کند (Wiley, McCormac & Calic 2020).

در این راستا پژوهش‌هایی از جمله Bauer & Bernroider (2017) و Bulgurcu, Cavusoglu & Benbasat (2010) نشان داده‌اند که ISA می‌تواند به بهبود رفتار امنیت اطلاعات و انطباق با خط‌مشی‌های امنیت اطلاعات منجر شود؛ برای نمونه، افزایش حفاظت از اطلاعات محرمانه Thomson & Von Solms (1998). همچنین در داخل ایران مهم‌ترین پژوهش‌هایی که به موضوع امنیت اطلاعات پرداخته‌اند، عبارت‌اند از: «پیکری و بنازاده» (۱۳۹۷)؛ «جعفری، حمیدی‌زاده و منتظری نجف‌آبادی» (۱۳۹۵)؛ «حسن‌زاده، کریم‌زادگان مقدم و جهانگیری» (۱۳۹۱)؛ «حسینی‌سنو و مظاهری» (۱۳۹۵)؛ «دهقانی» و همکاران (۱۳۹۸)؛ «کریمی و پیکری» (۱۳۹۷ و ۱۳۹۸). در میان آن‌ها تنها پژوهش «پیکری و بنازاده» مفهوم آگاهی از امنیت اطلاعات را مورد توجه قرار داده است. پژوهشگران در این پژوهش به بررسی رابطهٔ آگاهی از امنیت اطلاعات با قصد نقض امنیت اطلاعات با نقش میانجی هنجارهای فردی و خودکنترلی پرداخته‌اند. این پژوهش از نوع کاربردی و یک مطالعهٔ توصیفی-همبستگی است. جامعهٔ آن، ۳۵۰ نفر از کارکنان شعب بانک کشاورزی شهر اصفهان و نمونهٔ پژوهش با استفاده از جدول مورگان ۱۸۴ نفر هستند که با استفاده از روش نمونه‌گیری غیرتصادفی تعیین شده‌اند. یافته‌های این پژوهش نشان داد که آگاهی از امنیت اطلاعات با هنجارهای فردی و خودکنترلی، رابطه مثبت و معنادار و با قصد نقض امنیت اطلاعات، رابطهٔ منفی و معنادار دارد. افزون بر این، نتایج نشان دادند که هنجارهای فردی و خودکنترلی با قصد نقض امنیت اطلاعات رابطهٔ منفی و معنادار دارند (۱۳۹۷).

همچنین بررسی بانک‌های اطلاعاتی نشان می‌دهد که پژوهش‌های اندکی به

بررسی تأثیری که بی‌تفاوتی اخلاقی می‌تواند بر رفتارهای غیراخلاقی در یک سازمان داشته باشد، پرداخته‌اند. پژوهشگران در پژوهش Detert, Treviño & Sweitzer (2008) گرایش به بی‌تفاوتی اخلاقی را به رفتارهایی مانند تقلب، دروغ و دزدی ربط داده‌اند. افزون بر این، «آرکی و گرین» در پژوهش خود (D'Arcy et al. 2014) این مسئله را بررسی کردند که چگونه می‌توان از بی‌تفاوتی اخلاقی به‌عنوان مکانیسم مقابله‌ای برای رفع استرس ایجادشده توسط الزاماتِ پیچیده و مبهم امنیت اطلاعات استفاده کرد. در این پژوهش، پژوهشگران خاطرنشان کرده‌اند که بی‌تفاوتی اخلاقی، متغیرِ پیش‌بینِ خوبی برای نقض عمدی ISA محسوب می‌شود. با این حال، لازم است تأکید شود که پژوهش انجام‌شده فقط بر روی مجموعه‌ای محدود از تخلفات مربوط به ISA متمرکز بوده و سایر موارد مؤثر بر بی‌تفاوتی ISA، مانند دانش و نگرش ISA را مورد بررسی قرار نداده است (D'Arcy, J., & G. Greene. 2014). نتایج پژوهش‌های محدودی که در این زمینه وجود دارد، مُبین این است که بی‌تفاوتی اخلاقی، به‌ویژه جنبه‌هایی که به انتشار مسئولیت مربوط است، می‌تواند بر تعامل کارکنان با ISA تأثیرگذار باشد.

از سوی دیگر، رابطه بین فرهنگ سازمانی و فرهنگ امنیتی در پژوهش (Nosworthy 2000) تأیید شده و همچنین بین فرهنگ امنیتی و ISA از لحاظ نظری مورد تأیید قرار گرفته است (Da Veiga & Eloff 2010; Schlienger & Teufel 2003). با این حال، پژوهش‌های تجربی محدودی بر وجود این روابط صِحه گذاشته‌اند (Coopamootoo & Gross 2019). از جمله این پژوهش‌ها می‌توان به پژوهش انجام‌شده توسط «پارسونز» و همکاران اشاره کرد؛ یافته‌های این پژوهش که به روش کمی اکتشافی انجام شده، نشان‌دهندهٔ وجود رابطه‌ای مثبت بین ISA و فرهنگ امنیتی است. در این راستا کارکنان سازمان‌هایی که از فرهنگ امنیتی بهتری برخوردارند، به احتمال بیشتری از دانش، نگرش و رفتار مطابق با خط‌مشی‌ها و رویه‌های امنیت اطلاعات لازم برای حفظ امنیت اطلاعات در سازمان نیز برخوردارند (Parsons et al. 2015). این رابطه با پژوهش D'Arcy & Greene (2014) نیز پشتیبانی شده است.

همان‌طور که نشان داده شد، هر یک از پژوهش‌های یادشده بُعد خاصی از موضوع مورد بررسی را در نظر گرفته و آن را در مطالعه خود تشریح کرده‌اند. تعدادی از پژوهش‌ها تلاش کرده‌اند عوامل زمینه‌ساز آگاهی از امنیت اطلاعات را مورد بررسی قرار دهند و برخی دیگر، سازه‌های بی‌تفاوتی اخلاقی و فرهنگ سازمانی را مورد توجه قرار داده‌اند. در

این راستا بررسی‌ها نشان دادند که پژوهش‌های اندکی به بررسی تأثیری که بی‌تفاوتی اخلاقی می‌تواند بر رفتارهای غیراخلاقی در یک سازمان داشته باشد، پرداخته‌اند. بر اساس جست‌وجوی صورت گرفته، مشخص گردید که تاکنون سازه‌های بی‌تفاوتی اخلاقی، فرهنگ سازمانی و رفتارهای آگاهی از امنیت اطلاعات به‌صورت تجربی و به شکل ترکیبی و در قالب یک مدل مفهومی بررسی نشده‌اند. مقاله حاضر این شکاف تحقیقاتی را مورد بررسی قرار داده است. همچنین مشخص شد که استفاده از رویکرد حداقل مربعات جزئی به‌عنوان روش ارزیابی روابط بین متغیرهای مرتبط با رفتار انسان در حوزه امنیت اطلاعات، متداول‌ترین رویکرد در مطالعات کمی بوده است.

۳. مدل مفهومی و فرضیه‌ها

مدل پژوهش و متغیرهای این مطالعه (مطابق شکل ۱) بر اساس تلفیقی از مدل‌های ارائه‌شده در پژوهش‌های Hadlington, Binder & Stanulewicz (2021) و Wiley, McCormac & Calic (2020) و با بهره‌گیری از نظرات خبرگان طراحی شده است. مدل‌های ارائه‌شده در این پژوهش‌های با توجه به اینکه تأثیر بی‌تفاوتی اخلاقی و فرهنگ سازمانی بر آگاهی از امنیت اطلاعات را در جامعه‌ای متشکل از کارکنان صنایع مختلف که عمدتاً به‌صورت نیمه‌وقت شاغل بوده‌اند، مورد مطالعه قرار داده است، مناسب پژوهش حاضر در نظر گرفته شد. اما با در نظر گرفتن این جامعه، کارمندان بانک به‌عنوان یک هدف اصلی برای هکرهایی که قصد دسترسی به مناطق حساس سیستم‌های بانکی از طریق حملات سایبری را دارند، تا حدودی نادیده گرفته شده‌اند. در این رابطه و بر اساس شکل ۱، می‌توان فرضیه‌های پژوهش را به‌شرح زیر مطرح کرد:

فرضیه ۱. بی‌تفاوتی اخلاقی تأثیر منفی و معنادار بر رفتارهای آگاهی از امنیت اطلاعات کارکنان بانک‌های صادرات و ملت دارد.

فرضیه ۲. بی‌تفاوتی اخلاقی تأثیر منفی و معنادار بر دانش آگاهی از امنیت اطلاعات کارکنان بانک‌های صادرات و ملت دارد.

فرضیه ۳. بی‌تفاوتی اخلاقی تأثیر منفی و معنادار بر نگرش آگاهی از امنیت اطلاعات کارکنان بانک‌های صادرات و ملت دارد.

فرضیه ۴. دانش آگاهی از امنیت اطلاعات تأثیر مثبت و معنادار بر رفتارهای آگاهی از

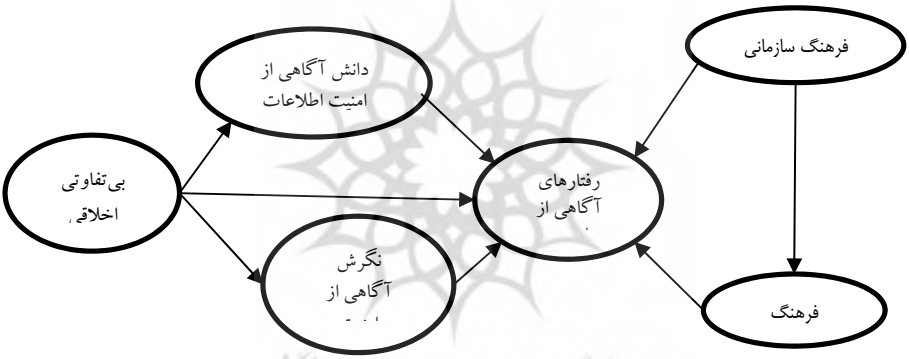
امنیت اطلاعات کارکنان بانک‌های صادرات و ملت دارد.

فرضیه ۵. نگرش آگاهی از امنیت اطلاعات تأثیر مثبت و معنادار بر رفتارهای آگاهی از امنیت اطلاعات کارکنان بانک‌های صادرات و ملت دارد.

فرضیه ۶. فرهنگ سازمانی تأثیر مثبت و معنادار بر رفتارهای آگاهی از امنیت اطلاعات کارکنان بانک‌های صادرات و ملت دارد.

فرضیه ۷. فرهنگ سازمانی تأثیر مثبت و معنادار بر فرهنگ امنیتی کارکنان بانک‌های صادرات و ملت دارد.

فرضیه ۸. فرهنگ امنیتی تأثیر مثبت و معنادار بر رفتارهای آگاهی از امنیت اطلاعات کارکنان بانک‌های صادرات و ملت دارد.



شکل ۱. مدل مفهومی پژوهش

(Wiley, McCormac & Calic 2020; Hadlington, Binder & Stanulewicz 2021)

٤. روش پژوهش

پژوهش حاضر از لحاظ هدف کاربردی محسوب می‌شود و از آنجا که هدف این پژوهش بررسی تأثیر بی‌تفاوتی اخلاقی و فرهنگ سازمانی بر رفتارهای مرتبط با آگاهی از امنیت اطلاعات با در نظر گرفتن نقش میانجی جنبه‌های شناختی-احساسی ISA (دانش و نگرش) و فرهنگ امنیتی سازمان است، توصیفی و از نوع همبستگی بوده و مبتنی بر مدل معادله‌های ساختاری است. جامعه آماری پژوهش کارکنان شعب بانک‌های ملت و صادرات در شهر تهران بودند. دلیل انتخاب بانک به‌منزله جامعه مطالعه این بود که کارمندان بانک به‌عنوان یک هدف اصلی برای هکرهایی محسوب می‌شوند که قصد

دسترسی به مناطق حساس سیستم‌های بانکی از طریق حملات سایبری دارند. در این راستا حجم نمونه بر اساس پیشنهاد پژوهشگران در پژوهش (Gay, Mills & Airasian 2012, p. 139) انتخاب شد که نشان دادند برای جمعیت‌های بیش از ۵۰۰۰ نفر، حجم جامعه دیگر بر اندازه نمونه تأثیر نمی‌گذارد و نمونه ۴۰۰ نفره کافی است. با توجه به اهمیت و حساسیت موضوع، پژوهشگران حجم نمونه را به ۴۳۰ نفر افزایش دادند. برای نمونه‌گیری از شیوه نمونه‌گیری طبقه‌بندی‌شده و با روش انتخاب تصادفی ساده استفاده شد. در این راستا پژوهشگران شهر تهران را به پنج بخش شمال، جنوب، شرق، غرب و مرکز تقسیم و سپس، از هر منطقه تعداد چهار شعبه (دو شعبه بانک صادرات و دو شعبه بانک ملت) به‌طور تصادفی انتخاب کردند و سرانجام، در هر شعبه به‌طور متوسط ۲۱ پرسشنامه را توزیع نمودند.

در ارتباط با ابزار پژوهش نیز بخش‌هایی از پرسشنامه‌های ارائه‌شده توسط Hadlington, Binder & Stanulewicz (2021) و Wiley, McCormac & Calic (2020) برای ارزیابی «بی‌تفاوتی اخلاقی» و «فرهنگ سازمانی» (متغیرهای مستقل)، «جنبه‌های دانش و نگرش آگاهی از امنیت اطلاعات» و «فرهنگ امنیتی» (متغیرهای میانجی) و «رفتارهای مرتبط با آگاهی از امنیت اطلاعات» (متغیر وابسته) استفاده شده است. پرسشنامه‌هایی که توسط آن‌ها آزمایش شده، متشکل از ۱۵۳ گویه هستند. بنابراین، با توجه به اینکه امکان داشت به‌دلیل تعدد سؤالات، برخی از اعضای نمونهٔ مورد مطالعه با دقت به سؤالات پاسخ ندهند، با مشورت اساتید، تعدادی از مهم‌ترین گویه‌ها (۵۶ گویه) برای درج در پرسشنامه استخراج گردید. لازم به ذکر است که در پرسشنامه مذکور از مقیاس ۷ درجه‌ای «لیکرت» بهره گرفته شده است. از میان پرسشنامه‌های ارسال‌شده، ۴۰۹ پرسشنامه دریافت شد، اما بعد از حذف پرسشنامه‌هایی که به‌صورت ناقص یا اشتباه پاسخ داده شده بودند، ۳۹۵ پرسشنامه برای تجزیه‌وتحلیل مورد استفاده قرار گرفت. لازم به ذکر است که پایایی ابزار پژوهش از طریق معیارهای آلفای کرونباخ و پایایی ترکیبی (جدول ۲) تأیید شد.

در این مطالعه برای تجزیه‌وتحلیل داده‌ها از روش تحلیل توصیفی با نرم‌افزار SPSS و رویکرد حداقل مربعات جزئی[1] با نرم‌افزار Smart PLS استفاده شده است. استفاده از رویکرد حداقل مربعات جزئی به‌عنوان روش ارزیابی روابط بین متغیرهای مرتبط با رفتار

1. partial least squares (PLS)

انسان در حوزه امنیت اطلاعات متداول‌ترین رویکرد در مطالعات کمی بوده است (برای نمونه، Hanus & Wu, 2016).

۵. یافته‌های پژوهش

یافته‌ها در دو بخش یافته‌های توصیفی (جمعیت‌شناختی) و یافته‌های تحلیلی گزارش شده‌اند.

۵-۱. یافته‌های توصیفی (جمعیت‌شناختی)

همان‌گونه که در جدول ۱، نشان داده شده، بیشتر پاسخ‌دهندگان مرد (۷۶ درصد) بودند؛ بزرگ‌ترین گروه از پاسخ‌دهندگان در بازه سنی بین ۲۵ تا ۳۵ سال (۴۶ درصد) قرار داشتند؛ بیشترین سابقه کار مربوط به بازه ۱۶ تا ۲۵ سال (۴۶ درصد) بود؛ و بیشتر پاسخ‌دهنگان دارای مدرک تحصیلی لیسانس بودند. یافته‌های مربوط به داده‌های جمعیت‌شناختی در جدول ۱، نشان داده شده است.

جدول ۱. داده‌های جمعیت‌شناختی

ویژگی‌ها		فراوانی	درصد
بانک	ملت	۲۰۴	۵۲
	صادرات	۱۹۱	۴۸
جنسیت	مرد	۲۹۹	۷۶
	زن	۹۶	۲۴
سن	۲۵-۳۵	۱۸۲	۴۶
	۳۶-۴۵	۱۵۷	۴۰
	۴۶ به بالا	۵۶	۱۴
سابقه کار	۵-۱۵	۱۷۱	۴۳
	۱۶-۲۵	۱۸۳	۴۶
	۲۶ به بالا	۴۱	۱۱

ویژگی‌ها		فراوانی	درصد
میزان تحصیلات	لیسانس	۲۵۲	۶۴
	فوق لیسانس	۱۰۲	۲۶
	دکتری	۴۱	۱۰

۵-۲. یافته‌های تحلیلی

روش PLS برای ارزیابی مدل‌های معادلات ساختاری، سه قسمت را تحت پوشش قرار می‌دهد: ۱) بخش مربوط به مدل اندازه‌گیری (مدل بیرونی)، ۲) بخش ساختاری (مدل درونی) و ۳) بخش کلی مدل (مدل اندازه‌گیری و ساختاری) (داوری و رضازاده ۱۳۹۵، ۸۸).

۵-۲-۱. ارزیابی مدل اندازه‌گیری (مدل بیرونی)

مدل بیرونی در روش PLS با مدل اندازه‌گیری در معادلات ساختاری مطابقت می‌کند. برای بررسی برازش مدل اندازه‌گیری PLS از پایایی شاخص، روایی همگرا و واگرا استفاده می‌شود.

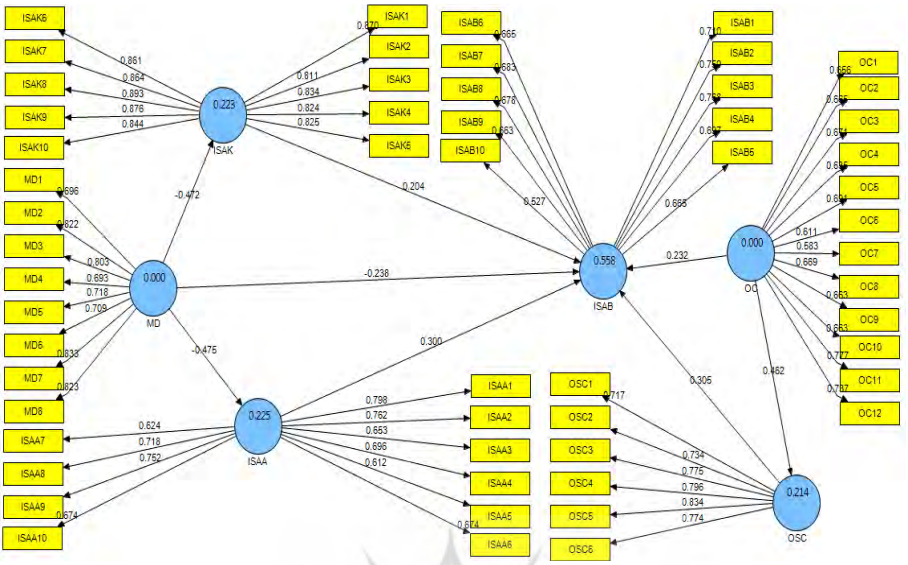
۵-۲-۱-۱. پایایی شاخص

در PLS، پایایی شاخص خود توسط سه معیار مورد سنجش قرار می‌گیرد: ۱) آلفای کرونباخ، ۲) پایایی ترکیبی، و ۳) ضریب بارهای عاملی. این شاخص‌ها در شکل ۲، و جدول ۲، ارائه شده‌اند. مطابق شکل ۲، در پژوهش حاضر تمامی سؤالات دارای بار عاملی بیش از ۰/۵ بودند.

۵-۲-۱-۲. روایی همگرا

روایی همگرا دومین معیاری است که برای برازش مدل‌های اندازه‌گیری در روش PLS به‌کار برده می‌شود و میزان همبستگی یک سازه با شاخص‌های خود را نشان می‌دهد. هرچه این همبستگی بیشتر باشد، برازش نیز بیشتر است. «فورنل و لارکر» معیار میانگین واریانس استخراج‌شده[1] را برای سنجش روایی همگرا معرفی کرده‌اند (Fornell & Larcker 1981). Magner, Welker & Campbell (1996) در پژوهش خود مقدار ۰/۴ به بالا را برای AVE کافی دانستند. مقادیر مرتبط با این شاخص نیز در جدول ۲، آورده شده است. همان‌طور که مشاهده می‌شود، این شاخص نیز برای تمامی متغیرها در سطح مناسب قرار دارد.

1. average variance extracted (AVE)



شکل ۲. ضرایب بار عاملی (تحلیل عاملی تأییدی)

(بی‌تفاوتی اخلاقی: MD، دانش آگاهی از امنیت اطلاعات: ISAK، نگرش آگاهی از امنیت: ISAA، رفتارهای آگاهی از امنیت: ISAB، فرهنگ سازمانی: OC، فرهنگ امنیتی: OSC)

جدول ۲. نتایج سه معیار آلفای کرونباخ، ضریب پایایی ترکیبی و روایی همگرا

متغیرهای مکنون	ضریب آلفای کرونباخ	ضریب پایایی ترکیبی	میانگین واریانس استخراجی
بی‌تفاوتی اخلاقی	۰/۸۹	۰/۹۱	۰/۵۸
دانش آگاهی از امنیت اطلاعات	۰/۹۵	۰/۹۶	۰/۷۲
نگرش آگاهی از امنیت اطلاعات	۰/۸۸	۰/۹۰	۰/۴۸
فرهنگ سازمانی	۰/۸۸	۰/۹۰	۰/۴۵
فرهنگ امنیتی سازمان	۰/۸۶	۰/۸۹	۰/۶۰
رفتارهای آگاهی از امنیت اطلاعات	۰/۸۷	۰/۸۹	۰/۴۶

۵-۲-۱-۳. روایی واگرا

روایی واگرا وقتی در سطح قابل قبول است که میزان AVE برای هر سازه بیشتر از واریانس اشتراکی بین آن سازه و سازه‌های دیگر (یعنی مربع مقدار ضرایب همبستگی بین سازه‌ها) در مدل باشد (Fornell & Larcker 1981). همان‌گونه که از جدول ۳، مشخص است، مقدار جذر AVE متغیرهای مکنون در پژوهش حاضر که در خانه‌های موجود در قطر اصلی

ماتریس قرار گرفته‌اند، از مقدار همبستگی میان آن‌ها که در خانه‌های زیرین و چپ قطر اصلی ترتیب داده شده‌اند، بیشتر است. از این‌رو، می‌توان اظهار داشت که در پژوهش حاضر، سازه‌ها (متغیرهای مکنون) در مدل، تعامل بیشتری با شاخص‌های خود دارند تا با سازه‌های دیگر. به بیان دیگر، روایی واگرای مدل در حد مناسبی است.

جدول ۳. شاخص روایی واگرا

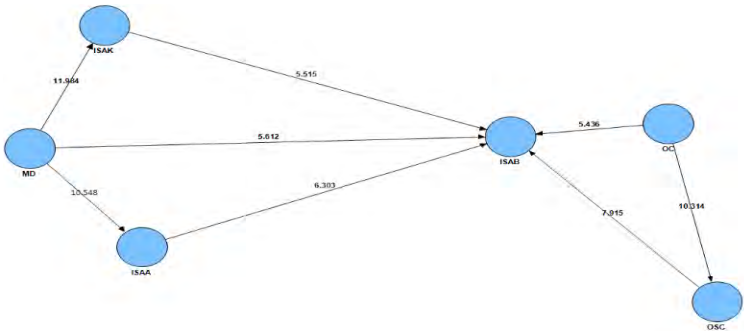
	فرهنگ امنیتی	فرهنگ سازمانی	بی‌تفاوتی اخلاقی	دانش آگاهی از امنیت اطلاعات	رفتارهای آگاهی از امنیت اطلاعات	نگرش آگاهی از امنیت اطلاعات
نگرش آگاهی از امنیت اطلاعات						۰/۶۹۲
رفتارهای آگاهی از امنیت اطلاعات					۰/۶۸۲	۰/۵۰۲۳۱۵
دانش آگاهی از امنیت اطلاعات				۰/۸۵۰	۰/۳۸۶۱۲۵	۰/۲۵۵۸۹۷
بی‌تفاوتی اخلاقی			۰/۷۶۴	−۰/۴۷۲۰۲۰	−۰/۴۶۲۷۳۶	−۰/۴۷۴۷۳۸
فرهنگ سازمانی		۰/۶۷۰	۰/۰۷۷۱۱۵	−۰/۰۶۶۴۸۸	۰/۳۶۴۹۷۱	۰/۰۷۹۸۸۶
فرهنگ امنیتی	۰/۷۷۲	۰/۴۶۲۰۸۱	−۰/۰۱۲۲۷۲	۰/۰۲۸۳۶۹	۰/۴۳۹۱۲۴	۰/۰۶۰۹۰۰

۵-۲-۲. برازش مدل ساختاری (مدل درونی)

پس از بررسی برازش مدل‌های اندازه‌گیری، نوبت به برازش مدل ساختاری پژوهش می‌رسد. بخش مدل ساختاری بر خلاف مدل‌های اندازه‌گیری، به سؤالات (متغیرهای آشکار) مربوط نیست و تنها متغیرهای پنهان همراه با روابط میان آن‌ها بررسی می‌شود (داوری و رضازاده ۱۳۹۵، ۱۴۱). اعداد معناداری t[1] و شاخص‌های برازش مدل درونی شامل R^2 و معیار Q^2 است. در صورتی که مقادیر اعداد معناداری t از ۱/۹۶ بیشتر شود، نشان از صحت رابطه بین سازه‌ها و مناسب بودن مدل ساختاری است (داوری و رضازاده ۱۳۹۵، ۹۰). R^2 معیاری است که نشان از تأثیر یک متغیر برون‌زا بر یک متغیر درون‌زا دارد و بیانگر این مطلب است که چه مقدار از متغیر وابسته توسط متغیر مستقل تبیین می‌شود. در پژوهش Chin (1998)، سه مقدار ۰/۱۹، ۰/۳۳ و ۰/۶۷ به‌عنوان مقدار ملاک برای مقادیر ضعیف، متوسط و قوی R^2 معرفی شده است. معیار Q^2 نیز قدرت پیش‌بینی مدل را مشخص

1. T- Values

می‌سازد. Henseler, Ringle & Sinkovics (2009) سه مقدار ۰/۰۲، ۰/۱۵ و ۰/۳۵ را به‌عنوان مقدار ملاک برای مقادیر ضعیف، متوسط و قوی Q^2 معرفی کرده‌اند.



شکل ۳. ضرایب معناداری

(بی‌تفاوتی اخلاقی: MD، دانش آگاهی از امنیت اطلاعات: ISAK، نگرش آگاهی از امنیت: ISAA، رفتارهای آگاهی از امنیت: ISAB، فرهنگ سازمانی: OC، فرهنگ امنیتی: OSC)

همان‌گونه که در شکل ۳، مشخص است، ضرایب معناداری مربوط به همه مسیرها از ۱/۹۶ بیشتر است، و این معنادار بودن مسیرها و مناسب بودن مدل ساختاری را نشان می‌دهد.

جدول ٤. شاخص‌های برازش مدل درونی پژوهش

سازه	ضریب R^2	معیار Q^2
نگرش آگاهی از امنیت اطلاعات	۰/۲۲۵	۰/۱۰
رفتارهای آگاهی از امنیت اطلاعات	۰/۵۵۸	۰/۲۵
دانش آگاهی از امنیت اطلاعات	۰/۲۲۳	۰/۱۵
فرهنگ امنیتی سازمان	۰/۲۱۴	۰/۱۲

همچنین با توجه به جدول ۴، می‌توان گفت که مقادیر R^2 و Q^2 مربوط به چهار متغیر درون‌زای فوق، در حد متوسط قرار دارند. بنابراین، برازش مناسب مدل ساختاری تأیید می‌شود.

۵-۲-۳. برازش مدل کلی (معیار GOF[1])

مدل کلی شامل هر دو بخش مدل اندازه‌گیری و ساختاری است و با تأیید برازش

1. Goodness of Fit

آن، بررسی برازش در یک مدل کامل می‌شود. مطابق فرمول زیر، نتایج مربوط به بررسی برازش مدل کلی نشان‌دهنده این است که با توجه به سه مقدار ۰/۰۱، ۰/۲۵ و ۰/۳۶ که به‌عنوان مقادیر ضعیف، متوسط و قوی برای GOF معرفی شده است (Wetzels, Odekerken-Schröder & Van Oppen 2009) و حصول مقدار ۰/۴۰۹، برازش بسیار مناسب مدل کلی تأیید می‌شود.

$$GOF=\sqrt{\overline{Communalities} \times \bar{R}^2}=\sqrt{\frac{0.488+0.466+0.723+0.584+0.449+0.596}{6} \times \frac{0.223+0.225+0.558+0.214}{4}}=0.409$$

شایان ذکر است که مقدار R^2 کلی برابر ۰/۵۵۸ است که نشان می‌دهد که مدل، ۵۵/۸ درصد از واریانس «رفتارهای آگاهی از امنیت اطلاعات» را توضیح می‌دهد. با مقایسه این یافته با یافته‌های Hadlington, Binder & Stanulewicz (2021) و Wiley, McCormac & Calic (2020) که به‌ترتیب دارای مقادیر R^2 برابر با ۳۵/۲۷ درصد و ۳۵ درصد بودند، می‌توان نتیجه گرفت که مدل بررسی‌شده در این پژوهش برای کارکنان بانک قوی‌تر است از کارکنان صنایع مختلف که عمدتاً به‌صورت نیمه‌وقت شاغل بوده‌اند. در حقیقت می‌توان این مدل را برای «کارکنان بانک»، قوی و برای «کارکنان صنایع مختلف و شاغل به‌صورت پاره‌وقت»، متوسط توصیف کرد. افزایش قدرت تبیینی مدل هنگامی که بر روی کارکنان بانک ارزیابی می‌شود، ممکن است با درک کارکنان بانک از تأثیر رفتارهای مرتبط با آگاهی از امنیت اطلاعات بر زندگی کاری و روزمره آن‌ها توضیح داده شود.

۵-۳. آزمودن فرضیه‌ها

با استفاده از مدل درونی می‌توان به بررسی فرضیه‌ها پرداخت. با مقایسه مقدار t محاسبه‌شده برای ضریب هر مسیر می‌توان به بررسی تأیید یا عدم تأیید فرضیه پژوهش پرداخت. بدین‌سان اگر مقدار آماره t بیشتر از ۲/۵۸ باشد، ضریب مسیر در سطح اطمینان ۹۹ درصد معنادار است. جدول شماره ۵، نتایج حاصل از فرضیه‌ها را در قالب ضرایب مسیر همراه با سطح معناداری نشان می‌دهد.

جدول ۵. نتایج آزمون فرضیه‌ها

ردیف	رابطه فرض‌شده	ضریب مسیر	آماره t	سطح معناداری	نتیجه آزمون
فرضیه اول	بی‌تفاوتی اخلاقی ← رفتارهای آگاهی از امنیت اطلاعات	۰/۲۳۸-	۵/۶۱۲	< ۰/۰۱	تأیید فرضیه
فرضیه دوم	بی‌تفاوتی اخلاقی ← دانش آگاهی از امنیت اطلاعات	۰/۴۷۲-	۱۱/۹۸۴	< ۰/۰۱	تأیید فرضیه
فرضیه سوم	بی‌تفاوتی اخلاقی ← نگرش آگاهی از امنیت اطلاعات	۰/۴۷۵-	۱۰/۵۴۸	< ۰/۰۱	تأیید فرضیه
فرضیه چهارم	دانش آگاهی از امنیت اطلاعات ← رفتارهای آگاهی از امنیت اطلاعات	۰/۲۰۴	۵/۵۱۵	< ۰/۰۱	تأیید فرضیه
فرضیه پنجم	نگرش آگاهی از امنیت اطلاعات ← رفتارهای آگاهی از امنیت اطلاعات	۰/۳۰۰	۶/۳۰۳	< ۰/۰۱	تأیید فرضیه
فرضیه ششم	فرهنگ سازمانی ← رفتارهای آگاهی از امنیت اطلاعات	۰/۲۳۲	۵/۴۳۶	< ۰/۰۱	تأیید فرضیه
فرضیه هفتم	فرهنگ سازمانی ← فرهنگ امنیتی	۰/۴۶۲	۱۰/۳۱۴	< ۰/۰۱	تأیید فرضیه
فرضیه هشتم	فرهنگ امنیتی ← رفتارهای آگاهی از امنیت اطلاعات	۰/۳۰۵	۷/۹۱۵	< ۰/۰۱	تأیید فرضیه

همان‌طور که در جدول ۴، مشاهده می‌شود، تأثیرگذاری متغیر «بی‌تفاوتی اخلاقی» بر متغیرهای «رفتارهای آگاهی از امنیت اطلاعات» (فرضیه اول)، «دانش آگاهی از امنیت اطلاعات» (فرضیه دوم) و «نگرش آگاهی از امنیت اطلاعات» (فرضیه سوم) به‌ترتیب با ضرایب مسیر ۰/۲۳۸-، ۰/۴۷۲- و ۰/۴۷۵- در سطح اطمینان برآوردشده منفی و معنادار است. همچنین تأثیر متغیر «دانش آگاهی از امنیت اطلاعات» بر «رفتارهای آگاهی از امنیت اطلاعات» (فرضیه چهارم)، تأثیر متغیر «نگرش آگاهی از امنیت اطلاعات» بر «رفتارهای آگاهی از امنیت اطلاعات» (فرضیه پنجم)، تأثیر متغیر «فرهنگ سازمانی» بر متغیرهای «رفتارهای آگاهی از امنیت اطلاعات» و «فرهنگ امنیتی سازمان» (فرضیه‌های ششم و هفتم) و تأثیر متغیر «فرهنگ امنیتی سازمان» بر «رفتارهای آگاهی از امنیت اطلاعات» (فرضیه هشتم) به‌ترتیب با ضرایب مسیر ۰/۲۰۴، ۰/۳۰۰، ۰/۲۳۲، ۰/۴۶۲ و ۰/۳۰۵ در سطح اطمینان برآوردشده مثبت و معنادار است. بنابراین، همه فرضیه‌های پژوهش تأیید می‌شوند.

۶. بحث و نتیجه‌گیری

با افزایش وابستگی جهان به داده‌های دیجیتال در هر جنبه‌ای از زندگی، اهمیت امنیت فناوری اطلاعات همچنان در حال افزایش است. فقدان سیستم‌های امنیتیِ کافی می‌تواند سازمان‌ها و افراد را در معرض نقض امنیت قرار دهد. این امر به‌نوبه خود

می‌توانـد پیامدهـای مخربـی به‌دنبـال داشـته باشـد. بـرای نمونـه، شـرکت «تارگـت»[1] در اثـر یـک رخنـه اطلاعاتـی میلیون‌هـا دلار از دسـت داد و ایـن رویـداد تأثیـر منفـی قابـل توجهـی بـر شـهرت آن شـرکت گذاشـت. بـا پیشـرفت سیسـتم‌های امنیتـی در واکنـش بـه شناسـایی امضاهـای حملـه[2]، هکرهـا تلاش‌هـای خـود را بـر روی ضعیف‌تریـن عنصـر زیرسـاخت امنیتـی یعنـی عنصـر انسـانی متمرکـز کرده‌انـد. بـر خـلاف راه‌کارهـای مبتنـی بـر فنـاوری کـه داده‌هـا را بـرای الگوهایـی کـه ظاهـر شـده یـا مخـرب شـناخته می‌شـوند، اسـکن می‌کننـد، انسـان‌ها در زمینه‌هایـی همچـون به‌کارگیـری سیسـتم‌های امنیتـی، پیـروی از خط‌مشـی‌ها و پاسـخ بـه حمـلات فیشـینگ و فیشـینگِ هدفمنـد متفـاوت هسـتند. بنابرایـن، بسـیار مهـم اسـت کـه بفهمیـم انسـان‌ها چگونـه در مواجهـه بـا ایـن ریسـک فزاینـده، بـرای بهبـود رفتـار خـود تـلاش می‌کننـد. ایـن فهـم بـرای هـر سـازمانی کـه ممکـن اسـت به‌واسـطهٔ از دسـت دادن اطلاعـات اختصاصـی، انتشـار اطلاعـات هویتیِ کارکنـان یـا مشـتریان، عـدم رعایـت الزامـات نظارتـی یـا حتـی دسترسـی بـه زیرسـاخت‌های محاسـباتی‌اش متأثـر شـود، بسـیار مهـم اسـت. در ایـن راسـتا، پژوهـش حاضـر به‌منظـور بررسـی تأثیـر بی‌تفاوتـی اخلاقـی و فرهنـگ سـازمانی بـر رفتارهـای مرتبـط بـا آگاهـی از امنیـت اطلاعـات بـا در نظـر گرفتـن نقـش میانجـی متغیرهـای شناختی-احساسـی و فرهنـگ امنیتـی در شـعب بانک‌هـای ملـت و صـادرات شـهر تهـران انجـام شـد.

در ایـن راسـتا، نتایـج تحلیـل معادلـه سـاختاری نشـان داد کـه فرضیه‌هـای اول، دوم و سـوم در سـطح اطمینـان برآوردشـده تأییـد می‌شـوند. نتایـج به‌دسـت‌آمده از پژوهـشِ حاضـر مبنـی بـر تأثیـر منفـی و معنـادار «بی‌تفاوتـی اخلاقـی» بـر متغیرهـای «رفتارهـای آگاهـی از امنیـت اطلاعـات»، «دانـش آگاهـی از امنیـت اطلاعـات» و «نگـرش آگاهـی از امنیـت اطلاعـات» بـا نتایـج پژوهـش Hadlington, Binder & Stanulewicz (2021) همسوسـت. در تبییـن ایـن فرضیـات می‌تـوان گفـت کـه احتمـالاً «بی‌تفاوتـی اخلاقـی» به‌عنـوان یـک مانـع اصلـی در برابـر پیـروی از پروتکل‌هـای امنیتـی عمـل می‌کنـد؛ چـرا کـه افـرادی کـه از روش‌هـای قانونـی، امـا غیراخلاقـی و نادرسـت بـرای دسـتیابی بـه اهـداف خـود در سـازمان اسـتفاده می‌کننـد، احتمـالاً نیـازی بـه درک و شـناخت خط‌مشـی‌های امنیـت اطلاعـات و تعامـل بـا اصـول امنیـت اطلاعـات در سـازمان نمی‌بیننـد و در نتیجـه، تـلاش چندانـی در ایـن جهـت نخواهنـد کـرد. لازم بـه ذکـر اسـت افـرادی کـه از سـطح بالایـی از بی‌تفاوتـی اخلاقـی برخوردارنـد، احتمـالاً نسـبت بـه مسـائل و مشـکلات سـازمان

1. Target
2. attack signatures

بی‌تفاوت بوده و درکشان از عدالت سازمانی نیز پایین است. از طرفی، در سازمان‌های بزرگ افراد با اتکا به حضور دیگران برای تحمل بار مسئولیت، احتمالاً راحت‌تر در زمینه «آگاهی از امنیت اطلاعات» شانه خالی می‌کنند.

همچنین نتایج تحلیل معادله ساختاری نشان داد که فرضیه‌های چهارم و پنجم در سطح اطمینان برآوردشده تأیید می‌شوند. نتایج به‌دست‌آمده از پژوهش حاضر مبنی بر تأثیر مثبت و معنادار متغیرهای «دانش آگاهی از امنیت اطلاعات» و «نگرش آگاهی از امنیت اطلاعات» بر «رفتارهای آگاهی از امنیت اطلاعات» با نتایج پژوهش Hadlington, Binder & Stanulewicz (2021) همسوست. در تبیین این فرضیات می‌توان گفت افرادی که دانش کافی و نگرش مناسبی نسبت به امنیت اطلاعات دارند، به‌دلیل اینکه از عواقب نقض امنیت اطلاعات و ضرورت رعایت خط مشی‌های امنیتی مطلع هستند، به احتمال زیاد رفتارهای مناسبی در زمینه امنیت اطلاعات از خود بروز خواهند داد.

در ارتباط با فرضیه ششم نیز نتایج تحلیل معادله ساختاری نشان داد که این فرضیه در سطح اطمینان برآوردشده تأیید می‌شود. نتایج به‌دست‌آمده از پژوهش حاضر مبنی بر تأثیر مثبت و معنادار متغیر «فرهنگ سازمانی» بر «رفتارهای آگاهی از امنیت اطلاعات» با نتایج پژوهش Wiley, McCormac & Calic (2020) همسوست. در تبیین این فرض می‌توان گفت از آنجا که امروزه دیگر امنیت اطلاعات صرفاً یک موضوع فنی نیست و مستلزم مشارکت کارکنان در رعایت و پیروی از خط‌مشی‌های سازمان در راستای حفظ امنیت اطلاعات است، بنابراین احتمالاً فرهنگ سازمانی که متشکل از باورها، ارزش‌ها و خط فکری کارکنان است، تعیین‌کننده رفتار کارکنان در این حوزه باشد. در فرضیه هفتم ادعا شده که «فرهنگ سازمانی» تأثیر مثبت و معنادار بر «فرهنگ امنیتی» سازمان دارد. نتایج تحلیل معادله ساختاری نشان داد که این فرضیه در سطح اطمینان برآوردشده تأیید می‌شود. نتایج به‌دست‌آمده از پژوهش حاضر مبنی بر تأثیر مثبت و معنادار متغیر «فرهنگ سازمانی» بر «فرهنگ امنیتی» با نتایج پژوهش‌های Da Veiga & Martins (2015) و Wiley, McCormac & Calic (2020) همسوست. در تبیین این فرض می‌توان گفت از آنجا که فرهنگ امنیتی زیرمجموعه‌ای از فرهنگ سازمانی است، احتمالاً با تقویت فرهنگ سازمانی، فرهنگ امنیتی نیز تقویت خواهد شد. در فرضیه هشتم ادعا شده که «فرهنگ امنیتی» تأثیر مثبت و معنادار بر «رفتارهای آگاهی از امنیت اطلاعات» دارد. نتایج تحلیل معادله ساختاری نشان داد که این فرضیه در سطح اطمینان برآوردشده تأیید می‌شود. نتایج به‌دست‌آمده از پژوهش

حاضر مبنی بر تأثیر مثبت و معنادار متغیر «فرهنگ امنیتی» بر «رفتارهای آگاهی از امنیت اطلاعات» با نتایج پژوهش‌های Da Veiga & Eloff (2010) و Wiley, McCormac & Calic (2020) همسوست. در تبیین این فرضیه می‌توان گفت افرادی که از سازمان‌هایی با فرهنگ امنیتی قوی‌تر هستند، احتمالاً امنیت را به‌عنوان یکی از ارکان اصلی سازمان پذیرفته و رعایت آن را نوعی ارزش محسوب می‌کنند. از طرفی، محیط سازمان نیز تفکرات امنیتی را ترویج می‌کند و این عوامل در رفتارهای کارکنان در حوزه امنیت اطلاعات تجلی و تبلور پیدا می‌کنند.

بر اساس یافته‌های فوق می‌توان گفت که بی‌تفاوتی اخلاقی منجر به کاهش ابعاد مختلف آگاهی امنیت اطلاعات می‌شود. بر این اساس، به‌منظور افزایش آگاهی امنیت اطلاعات کارکنان، کاهش بی‌تفاوتی اخلاقی ضروری است. جهت کاهش بی‌تفاوتی اخلاقی استفاده از مؤلفه‌های عدالت سازمانی و به‌کارگیری روش‌های اخلاقی برای حل تعارضات سازمانی بین رده‌های مختلف سازمان می‌تواند مفید واقع شود. از جمله این موارد می‌توان به رفتار منصفانه با کارکنان، تخصیص منصفانه پاداش‌ها، فراهم‌آوردن فرصت‌های ارتقا و محافظت از منافع کارکنان در بلندمدت اشاره کرد. از طرفی، با توجه به اینکه فرهنگ سازمانی عمیقاً درون یک سازمان نهادینه شده است، تغییر آن دشوار خواهد بود. با این حال، از آنجا که فرهنگ امنیتی زیرمجموعه‌ای از فرهنگ سازمانی است و قاعدتاً متمرکزتر است، احتمالاً مدیریت و تغییر آن آسان‌تر خواهد بود. در این راستا توصیه می‌شود سازمان‌ها با تمرکز بر درک و اصلاح فرهنگ امنیتی در جهت بهبود آگاهی امنیت اطلاعات کارکنان اقدام کنند و با این عمل از زمان و منابع خود به‌طور مؤثرتری استفاده خواهند کرد؛ چرا که تغییر گسترده فرهنگ نیازمند منابع بیشتری است که این امر زمان‌بر و پرهزینه خواهد بود. افزون بر این، تغییرات مثبت فرهنگی که آگاهی امنیت اطلاعات را بهبود می‌بخشند، ممکن است به بهبود فرهنگ کلی سازمان نیز منجرشود. بنابراین، توصیه می‌شود سازمان‌هایی که امیدوار به بهبود آگاهی امنیت اطلاعات هستند، به‌جای ایجاد تغییرات کلی در فرهنگ سازمانی، از طریق زیرساخت‌ها (برای نمونه، فنی و رویه‌ای) و هنجارهای گروهی (برای نمونه، سازوکارهایی مانند پشتیبانی مدیریت) بر فرهنگ امنیت تمرکز کنند.

۷. پیشنهادها

با توجه به اینکه این تحقیق در شُعب بانک‌های ملت و صادرات شهر تهران انجام شده و جامعه محدودی را دربرمی‌گیرد، به پژوهشگران علاقه‌مند به این موضوع توصیه می‌شود که این تحقیق را با همین ویژگی‌ها در سایر مؤسسات مالی نیز انجام دهند تا ضمن آشنایی با دیدگاه کارکنان بانک‌ها در سایر نقاط کشور، در صورت لزوم تصمیم‌های کلان در این مورد از سوی سیاست‌گذاران و مدیران مربوط گرفته شود. باید توجه داشت که با توجه به اینکه سعی شد اطلاعات به‌صورت کاملاً تصادفی از شعب بانک‌های ملت و صادرات شهر تهران جمع‌آوری شود، نتایج این پژوهش تنها به کارکنان بانک‌های مزبور در شهر تهران و سایر جوامعی که از نظر شرایط مختلف (جغرافیایی، مدیریتی، اندازه و ...) مشابه جامعه مورد بررسی هستند، قابل تعمیم است.

فهرست منابع

پیکری، حمیدرضا، و بابک بنازاده. ۱۳۹۷. رابطهٔ آگاهی از امنیت اطلاعات با قصد نقض امنیت اطلاعات با نقش میانجی هنجارهای فردی و خودکنترلی عنوان مکرر: قصد نقض امنیت اطلاعات. *پژوهش‌های راهبردی مسائل اجتماعی ایران* ۷ (۴): ۴۱–۵۸.

جعفری، سید محمدباقر، علی حمیدی‌زاده، و راضیه منتظری نجف‌آبادی. ۱۳۹۵. بررسی عوامل مؤثر بر پیروی کارکنان از سیاست‌های امنیت سیستم‌های اطلاعاتی در سازمان. *نشریه علمی مدیریت اطلاعات* ۲ (۲): ۱۰۲–۱۳۱.

حسن‌زاده، محمد، داود کریم‌زادگان مقدم، و نرگس جهانگیری. ۱۳۹۱. ارائه یک چارچوب مفهومی برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کاربران. *نظام‌ها و خدمات اطلاعاتی* ۱ (۲): ۱–۱۶.

حسینی‌سنو، سید امین، و الهام مظاهری. ۱۳۹۵. تأثیر حریم خصوصی، امنیت و اعتماد ادراک‌شده بر رفتار به اشتراک‌گذاری اطلاعات در شبکه‌های اجتماعی موبایل: نقش تعدیل‌کننده متغیر جنسیت. *پژوهشنامه پردازش و مدیریت اطلاعات* ۳۴ (۱): ۲۴۵–۲۷۴.

داوری، علی، و آرش رضازاده. (۱۳۹۵). *مدل‌سازی معادلات ساختاری با نرم‌افزار PLS*. تهران: نشر جهاد دانشگاهی.

دهقانی، محمد، زری رحمت‌پسند فتیده، زهرا آراسته، و کبری شکری‌زاده بزنجانی. ۱۳۹۸. آگاهی، نگرش و عملکرد کارکنان بخش مدیریت اطلاعات سلامت بیمارستان‌های ایران نسبت به امنیت اطلاعات سلامت. *مدیریت اطلاعات سلامت* ۱۶ (۱): ۳–۹.

کریمی، زهرا، و حمیدرضا پیکری. 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). *نشریه آموزش پرستاری* ۷ (۲): ۱۷–۲۴.

_____. ۱۳۹۸. مدیریت امنیت اطلاعات: تأثیر تعهد سازمانی و عواقب ادراک‌شده افشای اطلاعات محرمانه بر قصد نقض امنیت اطلاعات بیماران. *مجله اخلاق پزشکی* ۱۳ (۴۴): ۱–۱۰.

References

Baskerville, R., P. Spagnoletti, & J. Kim. 2014. Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management* 51 (1): 138–151.

Bauer, S., & E. W. N. Bernroider. 2017. From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 48 (3): 44–68.

Bulgurcu, B., H. Cavusoglu, & I. Benbasat. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* 34 (3): 523–548.

Chin, W. W. 1998. The partial least squares approach to structural equation modeling. *Modern Methods for Business Research* 295 (2): 295–336.

Coopamootoo, K., & T. Gross. 2019. A Systematic Evaluation of Evidence-Based Methods in Cyber Security User Studies. *School of Computing Technical Report Series* 5 (2): 241-260.

Cronk, L. 2017. Culture's influence on behavior: Steps toward a theory. *Evolutionary Behavioral Sciences* 11 (1): 36.

D'Arcy, J., & G. Greene. 2014. Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security* 22 (5): 474-489.

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

Da Veiga, A., & J. H. P. Eloff. 2010. A framework and assessment instrument for information security culture. *Computers & Security* 29 (2): 196–207.

Da Veiga, A., & N. Martins. 2015. Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review* 31 (2): 243–256.

Davidson, J. 2016. *FDIC reports five 'major incidents' of cybersecurity breaches since fall*. Washingtonpost. https://www.washingtonpost.com/news/powerpost/wp/2016/05/09/fdic-reports-five-major-incidents-of-cybersecurity-breaches-since-fall/ (accessed Jan. 11, 2021)

Detert, J. R., L. K. Treviño, & V. L. Sweitzer. 2008. Moral disengagement in ethical decision making: a study of antecedents and outcomes. *Journal of Applied Psychology* 93 (2): 374.

Ernst & Young Global Limited. 2019. *EY Global Information Security Survey 2018–19*. https://www.ey.com/Publication/vwLUAssets/EY_Global_Information_Security_Survey_2018/$FI%0ALE/EY Global Information Security Survey 2018-19.pdf (accessed March 25, 2021)

Fassihi, F., & R. Bergman. 2019. Iran Banks Burned, Then Customer Accounts Were Exposed Online. *The New York Times*. https://www.nytimes.com/2019/12/10/world/middleeast/Iran-bank-hacking-protests.html (accessed Dec. 9, 2020)

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

Gay, L. R., G. E. Mills, & P. W. Airasian. 2012. *Educational Research: Competencies for Analysis and Applications* (10th ed.). Pearson. https://yuli-elearning.com/mod/resource/view.php?id=677 (access Aug. 11, 2020)

Goldstein, J., A. Chernobai, & M. Benaroch. 2011. An event study analysis of the economic impact of IT operational risk and its subcategories. *Journal of the Association for Information Systems* 12 (9): 1.

Goodhue, D. L., & D. W. Straub. 1991. Security concerns of system users: A study of perceptions of the adequacy of security. *Information & Management* 20 (1): 13–27.

Guo, K. H. 2013. Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security* 32: 242–251.

Hadlington, L., J. Binder, & N. Stanulewicz. 2021. Exploring role of moral disengagement and counterproductive work behaviours in information security awareness. *Computers in Human Behavior*, *114*, 106557. https://doi.org/10.1016/j.chb.2020.106557 (accessed March 7, 2021)

Hadlington, L., & K. Parsons. 2017. Can cyberloafing and Internet addiction affect organizational information security? *Cyberpsychology, Behavior, and Social Networking* 20 (9): 567–571.

Hadlington, L., M. Popovac, H. Janicke, I. Yevseyeva, & K. Jones. 2019. Exploring the role of work identity and work locus of control in information security awareness. *Computers & Security* 81: 41–48.

Hanus, B., & Y. "Andy" Wu. 2016. Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management* 33 (1): 2–16.

Henseler, J., C. M. Ringle, & R. R. Sinkovics. 2009. The use of partial least squares path modeling in international marketing. *Advances in International Marketing* 20: 277–319. https://doi.org/10.1108/S1474-7979(2009)0000020014 (accessed Feb., 19 2020)

Höne, K., & J. H. P. Eloff. 2002. Information security policy—what do international information security standards say? *Computers & Security* 21 (5): 402–409.

Hsu, C., J. Backhouse, L. & Silva. 2014. Institutionalizing operational risk management: an empirical study. *Journal of Information Technology* 29 (1): 59–72.

Johnson, E. C. 2006. Security awareness: switch to a better programme. *Network Security* 2006(2): 15–18.

Kajzer, M., J. D'Arcy, C. R. Crowell, A. Striegel, & D. Van Bruggen. 2014. An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers & Security* 43: 64–76.

Magner, N., R. B. Welker, T. L. & Campbell. 1996. Testing a model of cognitive budgetary participation processes in a latent variable structural equations framework. *Accounting and Business Research* 27 (1): 41–50.

McCormac, A., D. Calic, K. Parsons, M. Butavicius, M. Pattinson, & M. Lillie. 2018. The effect of resilience and job stress on information security awareness. *Information & Computer Security* 26 (3): 277-289.

McCormac, A., T. Zwaans, K. Parsons, D. Calic, M. Butavicius & M. Pattinson. 2017. Individual differences and information security awareness. *Computers in Human Behavior* 69: 151–156.

Nctv. 2019. *Cybersecuritybeeld nederland*. https://www.thehaguesecuritydelta.com/media/com_hsd/report/237/document/CSBN2019-%0Aonline-tcm31-392768.pdf%0Awww.ncsc.nl (accessed Jan. 29, 2021)

Norton, J., & G. Walker. 2014. *Banks: fraud and crime*. ?: CRC Press.

Nosworthy, J. D. 2000. Implementing information security in the 21st century—do you have the balancing factors? *Computers & Security* 19 (4): 337–347.

Parsons, K. M., E. Young, M. A. Butavicius, A. McCormac, M. R. Pattinson, & C. Jerram. 2015. The influence of organizational information security culture on information security decision making.

Journal of Cognitive Engineering and Decision Making 9 (2): 117–129.

Pricewaterhouse Coopers. 2014. *Information Security Breaches Survey*. https://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf (accessed Dec. 28, 2020)

Schlienger, T., & S. Teufel. 2003. Analyzing information security culture: increased trust by an appropriate information security culture. *14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings.*, 405–409. Prague, Czech Republic

Siponen, M. T. 2000. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security* 8 (1): 31–41.

Siponen, M., & A. Vance. 2010. Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly* 34 (3): 487–502.

Stanton, J. M., K. R. Stam, P. Mastrangelo, & J. Jolton. 2005. Analysis of end user security behaviors. *Computers & Security* 24 (2): 124–133.

Tessem, H. M., & K. R. Skaaraas. 2005. Creating a security culture. *Telektronikk* 101 (1): 15.

Thomson, M. E., & R. Von Solms. 1998. Information security awareness: Educating your users effectively. *Information Management and Computer Security 6* (4): 167–173. https://doi.org/10.1108/09685229810227649

Warkentin, M., & R. Willison. 2009. Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems* 18 (2): 101–105.

Wetzels, M., G. Odekerken-Schröder, & C. Van Oppen. 2009. Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Quarterly* 33 (1): 177–195.

Wiley, A., A. McCormac, & D. Calic. 2020. More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security* 88: 101640.

تورج قهرمانی

متولد سال ۱۳۶۷ و دارای مدرک تحصیلی کارشناسی ارشد رشته مدیریت فناوری اطلاعات از دانشگاه پیام نور تهران است. ایشان هم‌اکنون در بخش تحقیقاتی یک سازمان دولتی مشغول به کار است. حوزه‌های مطالعاتی امنیت و دفاع سایبری، آینده‌پژوهی سایبری و روش‌شناسی پژوهش در زمینه مسائل سایبری از جمله علایق پژوهشی وی است.

فرهاد فرنیا

متولد سال ۱۳۶۳ و دانشجوی دکتری تخصصی مدیریت راهبردی فضای سایبر در دانشگاه عالی دفاع ملی است. ایشان هم‌اکنون با تخصص مدیریت سایبری در بخش دولتی مشغول به کار است.

مدیریت راهبردی، فضای سایبری و تدوین راهبردهای دفاعی از جمله علایق پژوهشی وی است.