ISSN: 3092-7196
E-ISSN: 2821-2304

Article history:
Received 29 April 2026
Accepted 30 May 2026
Published online 6 August 2026

Transformative Human Resources Quarterly
Homepage: https://sanad.iau.ir/journal/thr Volume: 5, Issue: 18, pp: 122-143

Behavioral Information Security in the Banking Sector: Integrating Psychological Capital into Protection Motivation Theory

Alireza Goli[1], Hamidreza Peikari*[2]

1. M.A. Graduate, Department of Public Administration, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran
2. Assistant Professor, Department of Communication Sciences and Business, Faculty of Humanities and Law, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran

Article Info

Article type:
Research Article

How to cite this article:

Goli, A.R, Peikari*, H.,R (2026). Behavioral Information Security in the Banking Sector: Integrating Psychological Capital into Protection Motivation Theory. Human Resources Quarterly, 5(18), 122-143.

Publisher:

Rafsanjan Islamic Azad University

ABSTRACT

Background and purpose: Information security within financial and banking institutions represents a critical, high-risk domain where employee behavior serves as a decisive factor in either mitigating or precipitating security breaches. While technical controls are indispensable, understanding the psychological drivers of compliance is essential for fostering proactive security habits. This study aims to evaluate the structural impact of psychological capital (PsyCap) on the formation of information security protection motivation, specifically examining the mediating mechanism of cognitive threat appraisal among banking professionals.

Research method: This study adopts an applied purpose and a descriptive-correlational research design. The target population comprised 1,320 employees of Bank Melli in Isfahan Province, from whom a sample of 297 respondents was selected via convenience sampling. Data were gathered using three standardized psychometric instruments measuring psychological capital, threat appraisal, and protection motivation. Structural Equation Modeling (SEM) based on the Partial Least Squares (PLS) approach was executed using SmartPLS software to validate the direct and indirect behavioral paths.

Findings: The empirical results indicate that psychological capital exerts a direct, positive, and statistically significant effect on both cognitive threat appraisal and information security protection motivation. Additionally, threat appraisal was confirmed as a robust direct predictor of protective intentions. Structural path analysis and mediation testing verified that threat appraisal functions as a significant mediator, channeling a substantial portion of psychological capital's total effect into active, voluntary protection motivation.

Conclusion: The findings indicated that strengthening employees' psychological capital can pave the way for increasing their sensitivity toward security threats and enhancing protective behaviors.

Keywords: *Psychological Capital (PsyCap), Threat Appraisal, Protection Motivation Theory (PMT), Behavioral Information Security*

NUMBER OF REFERENCES **33**

NUMBER OF FIGURES **0**

NUMBER OF TABLES **9**

Corresponding Author:
Email: omid726@yahoo.com
ORCID:000-0002-8754-3547

Introduction

In the contemporary digital landscape, information security presents a multifaceted challenge that transcends purely technical architectures. While firewalls, encryption protocols, and intrusion detection systems form vital lines of defense, the human element remains a critical vulnerability and a strategic asset. Emerging scholarship highlights that effective information security requires a balanced integration of technical controls and behavioral compliance.

Because employees throughout an enterprise must routinely access sensitive information systems, restricting user permissions excessively can stifle operational efficiency and organizational agility. This reality leaves organizations exposed to insider risk, where users may intentionally or unintentionally operate outside the boundaries of IT security protocols. Consequently, an organization's information security posture depends on Behavioral Information Security—the human actions and cognitive drivers that directly impact the availability, confidentiality, and integrity of data assets.

To bridge the gap between employee security awareness and actual compliant behavior, contemporary research is shifting toward positive organizational behavior. Rather than focusing purely on punitive measures or human errors, this study introduces Psychological Capital (PsyCap)—an intangible organizational resource comprising self-efficacy, hope, optimism, and resilience—as a foundational determinant of proactive security behavior. To model these effects, this study incorporates the motivational mechanics of Protection Motivation Theory (PMT). While traditional PMT models focus primarily on cognitive responses to threats, integrating PsyCap addresses a critical theoretical gap:

The Conceptual Integration: Psychological capital acts as a vital internal resource that shapes how individuals perceive and process external risks. Combining PsyCap with PMT honors the foundational premise that positive psychological resources enhance an individual's coping capacity without altering the underlying tenets of protection motivation. Furthermore, this study evaluates the mediating role of threat appraisal (the perceived severity of and vulnerability to a cyber risk) to understand the cognitive pathway through which an employee's psychological strengths translate into active information security protection motivation.

Research Methodology

This study utilizes an applied, empirical research design executed through a descriptive-correlational survey methodology.

- Target Population and Sample: The study population comprised all N = 1,320$ employees across Bank Melli branches in Isfahan Province. Employing convenience sampling based on organizational accessibility, a sample of n = 297 respondents was secured. The sample size was validated against Morgan's sample determination matrices to ensure robust statistical power.
- Measurement Instruments: Data were collected using three structurally validated, Likert-scale instruments:
    1. Luthans' Psychological Capital Questionnaire (PCQ): Adapting dimensions of self-efficacy, hope, resilience, and optimism.
    2. Workman's Threat Appraisal Scale: Measuring perceived severity and vulnerability.

3. Posey's Protection Motivation Questionnaire: Assessing voluntary intentions to safeguard information assets.

- Data Analysis Strategy: Structural Equation Modeling via Partial Least Squares (PLS-SEM) was executed using SmartPLS software. PLS-SEM was selected for its superior performance in analyzing complex hierarchical path models, handling latent psychological constructs, and managing non-normally distributed data profiles. Instrument reliability and validity were confirmed through Cronbach's alpha, Composite Reliability (CR), Average Variance Extracted (AVE), and the Fornell–Larcker discriminant validity criterion.

Findings

The structural path analysis revealed significant direct and indirect relationships among the latent variables, validating the hypothesized psychological path to cybersecurity compliance. The structural equations and mediation metrics yielded the following statistical relationships:

Independent Variable	**Mediator**	**Dependent Variable**	**Structural Metric / Index**	**Statistical Significance & Result**
Psychological Capital	—	Threat Appraisal	Path Coefficient ($\beta > 0$)	Statistically Significant (Direct Effect)
Psychological Capital	—	Protection Motivation	Path Coefficient ($\beta > 0$)	Statistically Significant (Direct Effect)
Threat Appraisal	—	Protection Motivation	Path Coefficient ($\beta > 0$)	Statistically Significant (Direct Effect)
Psychological Capital	Threat Appraisal	Protection Motivation	$VAF = 0.611$ / $Z = 3.126$	**Significant Partial Mediation**

Core Empirical Insights:

- PsyCap as a Perceptual Filter: Psychological capital exerts a direct, positive impact on an employee's threat appraisal. This indicates that employees with high self-efficacy, optimism, resilience, and hope do not ignore risks; rather, they demonstrate a superior cognitive capacity to accurately recognize the severity of cyber threats and assess institutional vulnerability.
- Direct Behavioral Motivation: Higher levels of internal PsyCap directly predict stronger protection motivation. Empowered employees show a greater baseline intention to adhere to security policies and avoid risky behaviors.
- The Power of Cognitive Mediation: Threat appraisal emerged as a strong predictor of protective intentions. Crucially, mediation analysis backed by a Sobel test Z-statistic of $Z = 3.126$ and a Variance Accounted For index of $VAF = 0.611$ confirmed that threat appraisal partially mediates the relationship. Substantively, over 61% of the total effect of an employee's psychological capital on their security protection motivation is transmitted indirectly through the cognitive mechanism of threat appraisal.

Conclusion

Theoretically, this study extends Protection Motivation Theory by establishing psychological capital as a critical, distal cognitive antecedent that drives the threat appraisal process. It demonstrates that positive psychological resources are foundational in determining how employees evaluate risk. From a practical

and managerial standpoint, these findings prove that relying solely on technical constraints or dry, policy-oriented compliance memos is insufficient to build a secure corporate culture. Because human behavior is heavily influenced by internal psychological states, financial institutions must shift toward a human-centric security paradigm.

To operationalize these insights within high-risk financial environments like Bank Melli, human resource and cybersecurity directors should implement the following targeted initiatives:

- Incorporate POB into Security Awareness: Integrate Positive Organizational Behavior (POB) workshops with traditional cybersecurity drills. Training should simultaneously build technical threat-recognition skills and boost employees' situational self-efficacy and resilience.
- Design Constructive Threat Communications: Avoid paralyzing, fear-inducing security compliance messages. Instead, structure threat alerts to frame cybersecurity as a shared, achievable responsibility, reinforcing employee optimism and proactive problem-solving.
- Utilize Cognitive Conduits for Behavioral Change: Recognize that building an employee's psychological resilience directly clarifies their risk perception (VAF = 0.611). Security programs should actively measure and develop psychological capital during routine performance reviews to maintain a strong human firewall.

In conclusion, cultivating psychological capital provides a cost-effective, sustainable strategy to strengthen employee threat appraisal and maximize information protection motivation. By intentionally linking psychological development with cybersecurity education, financial institutions can systematically mitigate human-induced vulnerabilities and foster a resilient, proactive security culture.

AUTHOR CONTRIBUTIONS

Conceptualization: Alireza Goli; Methodology: Hamidreza Pikari; Formal Analysis: Hamidreza Pikari; Writing – Original Draft: Alireza Goli; Writing – Review & Editing: All authors; Supervision: Hamidreza Pikari.

ACKNOWLEDGEMENT

The authors received no specific funding for this work. We appreciate the anonymous reviewers for their insightful comments.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

PUBLISHER'S NOTE

The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

POSITIVE AI STATEMENT

Artificial Intelligence Statement: Artificial intelligence (AI) tools, including large language models, were used solely for language editing and improvement of readability in this manuscript. The AI was not used for generating ideas, data analysis, interpretation of results, or writing the scientific content. All intellectual contributions and scientific decisions

ABBREVIATIONS

PsyCap = Psychological Capital PM = Protection Motivation PMT = Protection Motivation Theory IS / InfoSec = Information Security

AUTHOR(S) BIOSKETCHES

Hamidreza Pikari is an Assistant Professor in the Department of Communication and Business Sciences at Islamic Azad University, Isfahan (Khorasgan) Branch, Isfahan, Iran. He also serves as a member of the editorial board of the *Journal of Business Data Science Research*. His research interests include organizational behavior, and business development. Corresponding author: Email: omid726@yahoo.com

شاپا : ۳۰۹۲-۷۱۹۶
شاپای الکترونیکی: ۲۳۰۴-۲۸۲۱

تاریخچه مقاله :
دریافت شده در تاریخ ۹ اردیبهشت ۱۴۰۵
پذیرفته شده در تاریخ ۹ خرداد ۱۴۰۵
منتشر شده در تاریخ ۱۵ مرداد ۱۴۰۵

فصلنامه منابع انسانی تحول آفرین

دوره ۵، شماره ۱۸، صفحه ۱۴۳-۱۲۲ Homepage: https://sanad.iau.ir/journal/thr

تبیین انگیزه حفاظت از امنیت اطلاعات بر اساس سرمایه روان‌شناختی و ارزیابی تهدید در کارکنان بانکی

علیرضا گلی*[۱]، حمیدرضا پیکری[۲]

۱. دانش آموخته کارشناسی ارشد، گروه مدیریت دولتی، واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، اصفهان، ایران
۲. استادیار گروه علوم ارتباطات و کسب کار، دانشکده علوم انسانی و حقوق، دانشگاه آزاداسلامی، احداصفهان(خوراسگان)، اصفهان، ایران

اطلاعات مقاله

نوع مقاله:
مقاله پژوهشی

نحوه استناد به مقاله:

گلی*، ع . پیکری ،ح.ر (۱۴۰۵). تبیین انگیزه حفاظت از امنیت اطلاعات بر اساس سرمایه روان‌شناختی و ارزیابی تهدید در کارکنان بانکی. فصلنامه منابع انسانی تحول آفرین، ۵ (۱۸)، ۱۴۳-۱۲۲.

ناشر:
دانشگاه آزاد اسلامی رفسنجان

چکیده

زمینه و هدف: امنیت اطلاعات در سازمان‌های مالی و بانکی یکی از مهم‌ترین حوزه‌های پرریسک است و رفتار کارکنان نقش تعیین‌کننده‌ای در بروز یا پیشگیری از تهدیدهای امنیتی دارد. شناخت عوامل روان‌شناختی مؤثر بر انگیزه حفاظت از اطلاعات می‌تواند به ارتقای رفتارهای حفاظتی کارکنان منجر شود. هدف این پژوهش تبیین نقش سرمایه روان‌شناختی در شکل‌گیری انگیزه حفاظت از امنیت اطلاعات با تأکید بر نقش میانجی ارزیابی تهدید در میان کارکنان بانکی می باشد.

روش تحقیق: تحقیق حاضر از نوع کاربردی و با روش توصیفی- همبستگی انجام شد. جامعه آماری شامل کارکنان بانک ملی استان اصفهان به تعداد ۱۳۲۰ نفر بود که از میان آنان ۲۹۷ نفر به روش نمونه‌گیری مناسب انتخاب شدند. داده‌ها با استفاده از سه پرسشنامه جمع‌آوری شد. تحلیل داده‌ها با استفاده از نرم‌افزار SmartPLS و رویکرد مدل‌یابی معادلات ساختاری انجام گرفت.

یافته‌ها: نتایج نشان داد سرمایه روان‌شناختی اثر مثبت و معناداری بر ارزیابی تهدید و انگیزه حفاظت از امنیت اطلاعات دارد. همچنین ارزیابی تهدید نیز پیش‌بینی‌کننده معنادار انگیزه حفاظت بود. آزمون اثر غیرمستقیم نشان داد ارزیابی تهدید نقش میانجی معناداری در رابطه بین سرمایه روان‌شناختی و انگیزه حفاظت ایفا می‌کند.

نتیجه گیری: نتایج نشان داد تقویت سرمایه روان‌شناختی کارکنان می‌تواند زمینه‌ساز افزایش حساسیت آنان نسبت به تهدیدهای امنیتی و ارتقای رفتارهای حفاظتی شود.

واژه های کلیدی: *سرمایه روان‌شناختی، ارزیابی تهدید، انگیزه حفاظت، امنیت اطلاعات، نظریه انگیزه حفاظت*

* نویسنده مسئول:
ایمیل: ba.kargar@iau.ac.ir
ORCID: 0000-0002-0682-0275

مقدمه

یکی از چالش های مدیریتی و فنی در مسیر امنیت اطلاعات، سرمایه روانشناختی پرسنل و انگیزه ایشان در حفاظت از امنیت اطلاعات می باشد (بارنز[1] و همکاران، ۲۰۱۷)، چرا که دیدگاه هایی وجود دارد که نشان دهنده این موضوع هستند که حفاظت از امنیت اطلاعات به صورت کارآمد، به یک مولفه رفتاری و فنی نیاز دارد (الهوجیل[2]، ۲۰۱۵)، درواقع توجه به ملاحظات رفتاری[3] کارکنان در امنیت سیستم های اطلاعاتی[4]، به موضوعی محوری تبدیل گشته است که در کل سازمان، کارکنان به سیستم های اطلاعاتی سازمانی از طرق مختلف دسترسی دارند (کیسکو[5]، ۲۰۱۳) و دسترسی وسیع کارکنان به برخی از سیستم ها، سبب ایجاد محیط امنیتی ناسالم و پیچیده می گردد که ممکن است باعث از بین رفتن امنیت اطلاعات شود چرا که کاربران می توانند فراتر از کنترل سیستم امنیت فناوری اطلاعات عمل کنند و متأسفانه در برخی مواقع نیز به جهت اثربخشی سازمانی، نمی توان دسترسی کاربران به این سیستم ها را محدد نمود(وانس[6] و همکاران، ۲۰۱۵).

بنابراین، برخی از محققان امنیت اطلاعات بیان داشته اند که امنیت اطلاعات سازمان به تلاش های امنیتی کارکنان درون سازمانی بستگی دارد که به سیستم های اطلاعاتی شرکت دسترسی دارند(هسیو[7] و همکاران، ۲۰۱۵). این کارکنان تمام وقت و پاره وقت و همچنین از عاملان مجاز شرکت بوده که به دارایی های اطلاعاتی سازمان دسترسی دارند(پوزی[8] و همکاران، ۲۰۱۳). بنابراین با وجود چنین کارکنانی، مفهومی به نام امنیت اطلاعات رفتاری[9] ظهور نمود که شامل اقدامات انسانی می باشد که بر در دسترس بودن، محرمانه بودن و یکپارچگی سیستم های اطلاعات تاثیر می گذارند(استانتون[10] و همکاران، ۲۰۰۶).

برای پرداختن به مرز بین دانش کارکنان داخلی و توانایی های آنها در رفتارهای امنیتی، نیاز به یک بینش روانشناسانه مثبت برای تقویت درک بهتر احساس می شود (گابلی و هایت[11]، ۲۰۰۵)، روانشناسی مثبت شاخه ای از روان شناسی است که عملکرد بهینه افراد، گروه‌ها و نهادها را مورد توجه قرار می دهد و به دنبال بهبود کارهای صحیح نسبت به کارهایی که اغلب در مردم به صورت اشتباه تثبیت شده می باشد(شلدون و کینگ[12]، ۲۰۰۱). اصول اساسی روانشناسی مثبت؛ امید، انعطاف پذیری، خوش بینی و خودکارآمدی می باشند. درواقع روانشناسی مثبت به دلیل تاکید بر عملکرد مثبت رفتارهای افراد، آنها را به خوبی برای تلاش در جهت تحقق افزایش حفاظت اطلاعات، برمی انگیزاند و به صورت یک مکمل ایده آل برای تحقق

1 Burns
2 AlHogail
3 Behavioral considerations
4 IS security
5 Cisco
6 Vance
7 Hsu
8 Posey
9 behavioral information security
10 Stanton
11 Gable & Haidt
12 Sheldon & King

حفاظت سیستم اطلاعات عمل می کند (بارنز و همکاران، ۲۰۱۷) و در نتیجه، یکپارچگی روانشناختی مثبت با رویکردهای فعلی امنیت سیستم های اطلاعاتی و تفسیر آنها می تواند، نتایج مربوط به امنیت را بهبود دهد، بخصوص نتایجی که مستقیما ناشی از رفتارهای کارکنان است. برای نشان دادن نقش روانشناختی مثبت در امنیت سیستم های اطلاعاتی، جنبه های انگیزشی از چارچوب انگیزشی تئوری انگیزه حفاظت[1] ارزیابی می شود (ریپیتو و راجرز [2]، ۱۹۸۷).

سرمایه روان شناختی مانند سرمایه انسانی و سرمایه اجتماعی از سرمایه های ناملموس سازمانی است که برخلاف سرمایه های ملموس با هزینه های کمتر قابل مدیریت و رهبری می باشد و می تواند نتایج و دستاوردهای درخور توجهی را در پی داشته باشد (لوتانز[3] و همکاران، ۲۰۰۷)، سرمایه روان شناختی با تکیه بر مؤلفه های روان شناختی مثبت گرا، منجر به ارتقای ارزش سرمایه انسانی و اجتماعی در سازمان می شود. این مؤلفه ها در یک فرآیند تعاملی و با رویکرد ارزشیابی به زندگی فرد معنا می بخشد، تلاش فرد برای تغییر موقعیت های فشارزا را تداوم می دهد و او را برای ورود به صحنه عمل آماده، مقاومت و سرسختی وی در تحقق اهداف را تضمین می کند (ضیا و همکاران، ۱۳۹۳)، بنابراین استفاده از سرمایه روانشناختی در تحقق امنیت سیستم اطلاعاتی سازمانی می تواند بسیار مؤثر باشد (پارکر[4]، ۱۹۹۸). یکپارچگی سرمایه روانشناختی با نظریه انگیزه حفاظت مطابق با دیدگاه بنیان گذاران تئوری انگیزه حفاظت می باشد و بیان می کند توجه به نتایج مثبت کار، سبب بهبود کاربردپذیری این تئوری بدون اصلاح اصول آن می شود (موداکس و راجرز[5]، ۱۹۹۸). بدین ترتیب، بررسی رفتارهای سرمایه روانشناختی در مقابله با تهدیدها، که در این پژوهش با عنوان تئوری انگیزه حفاظت مطرح می شوند عملکرد کارکنان در انجام اقدامات مبتنی بر حفاظتی مانند رفتارهای انگیزش حفاظت[6] را نشان می دهد و درواقع تئوری انگیزه حفاظت شامل رفتارهای ارادی کارکنان است که برای حفاظت اطلاعات و سیستم های اطلاعاتی انجام می گردد (پوزی و همکاران، ۲۰۱۳).

محققان و پژوهشگران در جریان این تحقیق تئوری معروف به حفاظت اطلاعات یا تئوری انگیزاننده حفاظت توسعه داده شده است که شامل روابط سرمایه روانشناختی با عوامل انگیزاننده حفاظت می باشد. سرمایه روانشناختی نیز یک ساختار از نقش وسیع ظرفیت های روان شناختی و منابع در بر دارنده منابع انگیزشی مهم مربوط به روابط کاری می باشد، همچنین تحقیقات نشان دادند که می‌توان سرمایه روانشناختی را توسعه داد، در نتیجه با توجه به ارتباط نقش سرمایه روانشناختی با عوامل انگیزاننده حفاظت یک انگیزه قبلی و مهم و قابل انعطاف به وجود آمده است که مکمل عوامل انگیزاننده حفاظت می باشد که در بیشتر ارزیابی های معاصر مدل انگیزاننده حفاظت مفهوم شده است(فیروز بخت و همکاران، ۱۳۹۶). همچنین برخی از پژوهش ها همچون پژوهش بانز و همکاران(۲۰۱۷) نشان دادند که متغیر ارزیابی تهدید می تواند در رابطه بین این دو متغیر نقش میانجی دارد، درواقع بین ادراک ارزیابی تهدید و سرمیه روان شناختی از طریق رابطه زیر ساخت های ظرفیت روانی با

1 protection motivation theory (PMT)
2 Rippetoe & Rogers
3 Luthans
4 Parker
5 Maddux & Rogers
6 protection-motivated behaviors(PMBs)

تصورات مربوطه رابطه وجود دارد و هنگامی که سرمایه روانشناختی با تهدید مواجه می شوند به ارزیابی تهدیدات در مورد تاثیرات بالقوه آن برسازمان و امنیت اطلاعات می پردازند و نهایتا ارزیابی تهدید مقدمه ای بر برانگیزاندن انگیزه حفظات از امنیت اطلاعات سرمایه روانشناختی می گردد.

در دهه‌های اخیر، گسترش زیرساخت‌های فناورانه و دیجیتالی‌شدن خدمات سازمانی، به‌ویژه در صنعت بانکداری، وابستگی سازمان‌ها به امنیت اطلاعات را بیش از پیش افزایش داده است. اگرچه توسعه ابزارهای فنی نقش مؤثری در کاهش تهدیدات سایبری داشته است، پژوهش‌های جدید نشان می‌دهند که عامل انسانی همچنان مهم‌ترین نقطه آسیب‌پذیری در اغلب رخدادهای نقض داده است (انور[1] و همکاران، ۲۰۲۰). کارکنان سازمان‌ها، آگاهانه یا ناآگاهانه، می‌توانند موجب بروز رفتارهای پرخطر، بی‌توجهی به سیاست‌های امنیتی یا تبعیت ناقص از دستورالعمل‌های حفاظت از داده شوند. این مسئله سبب شده است که تمرکز پژوهش‌ها از «فناوری‌محوری» به «رفتارمحوری» تغییر یابد.

در سال‌های اخیر، نظریه انگیزش حفاظت به عنوان چارچوبی معتبر برای تبیین رفتارهای امنیت اطلاعات مطرح شده است. این نظریه بر دو مؤلفه «ارزیابی تهدید» و «ارزیابی راهبرد مقابله» تأکید دارد و بیان می‌کند که اگر کارکنان تهدید را محتمل و جدی تلقی کنند و پیامدهای آسیب را بالا برآورد نمایند، احتمال توجه به توصیه‌های امنیتی افزایش می‌یابد (ایفینیدو[2]، ۲۰۱۹). در حوزه بانکداری، این سازوکار اهمیت بیشتری دارد؛ چون کارکنان به‌طور روزانه با داده‌های حساس مالی مواجه‌اند. با این حال، تحقیقات جدید نشان می‌دهند که فرآیندهای شناختی–هیجانی کارکنان تنها در حضور منابع روان‌شناختی مثبت فعال می‌شوند. در اینجا مفهوم سرمایه روان‌شناختی که شامل امید، تاب‌آوری، خودکارآمدی و خوش‌بینی است، اهمیت پیدا می‌کند. پژوهش‌های اخیر ثابت کرده‌اند که کارکنانی که از سرمایه روان‌شناختی بالاتری برخوردارند، تهدیدها را دقیق‌تر ادراک می‌کنند، رفتارهای پیش‌نگرانه بیشتری دارند و در برابر فشارهای محیطی، عملکرد مطلوب‌تری نشان می‌دهند (ژانگ[3] و همکاران، ۲۰۲۳؛ کیم و کوسکه[4]، ۲۰۲۲). ازاین‌رو، ترکیب سرمایه روان‌شناختی با رفتارهای انگیزش حفاظت می‌تواند الگوی مفهومی قدرتمندی برای تبیین رفتارهای امنیت اطلاعات ارائه کند.

مبانی نظری

سرمایه روان‌شناختی

سرمایه روان‌شناختی بر اساس مدل لوتانز و یوسف–مورگان مجموعه‌ای از چهار مؤلفه مثبت‌نگر شامل خودکارآمدی، امید، خوش‌بینی و تاب‌آوری است. این سازه به عنوان یک توانمندی قابل‌توسعه، نقش مهمی در ارتقای رفتارهای سازگار در

1 Anwar
2 Ifinedo
3 Zhang
4 Kim & Koeske

محیط‌های پیچیده سازمانی دارد. پژوهش‌ها نشان می‌دهند که کارکنان با بالا انرژی روانی بیشتری برای مقابله با تهدیدات سازمانی دارند و در مواجهه با شرایط فشارزا، تصمیمات سازنده‌تری اتخاذ می‌کنند (لوتانز و یوسف–مورگان[1]، ۲۰۲۲). مطالعات جدید حوزه امنیت سایبری نشان می‌دهند که سرمایه روانشناختی می‌تواند رفتارهای تبعیت امنیتی را از طریق افزایش انگیزش درونی، احساس توانمندی و مدیریت هیجان‌های منفی تقویت کند. به‌عنوان مثال، کیم و کوسکه (۲۰۲۲) نشان دادند که سرمایه روانشناختی به‌طور معناداری پایبندی کارکنان به سیاست‌های امنیت اطلاعات را پیش‌بینی می‌کند.

ارزیابی تهدید

در نظریه انگیزش حفاظت، ارزیابی تهدید شامل دو مؤلفه احتمال وقوع تهدید و شدت پیامدهای آن است. کارکنانی که حساسیت بیشتری نسبت به پیامدهای نقض امنیت دارند، رفتارهای محافظتی بیشتری اتخاذ می‌کنند. یافته‌های اخیر نشان می‌دهند که در محیط‌های مالی، تجربه قبلی کارکنان و ادراک آنان از پیامدهای قانونی و اعتباری نقض داده‌ها، ارزیابی تهدید را تقویت می‌کند (ایفینیدو، ۲۰۱۹). نکته مهم آن است که ارزیابی تهدید تنها یک فرایند شناختی نیست، بلکه در تعامل با منابع هیجانی و روان‌شناختی شکل می‌گیرد. بر اساس پژوهش ژانگ و همکاران (۲۰۲۳)، سرمایه روان‌شناختی مثبت باعث می‌شود کارکنان تهدیدها را واقعی‌تر و دقیق‌تر تفسیر کنند.

انگیزش حفاظت

انگیزش حفاظت یک سازه کلیدی در رفتارهای انگیزش حفاظت است که بر قصد فرد برای انجام رفتار محافظتی دلالت دارد. این انگیزش زمانی فعال می‌شود که فرد: تهدید را مهم و شدید تلقی کند، توانایی مقابله با آن را در خود ببیند، و انتظار داشته باشد که اقدام محافظتی سودمند است. مطالعات متعدد نشان داده‌اند که انگیزش حفاظت پیش‌بینی‌کننده اصلی رفتارهای امنیت اطلاعات، از جمله استفاده ایمن از سامانه‌ها، رعایت سیاست‌های امنیتی و خودنظارتی است (انور و همکاران، ۲۰۲۰).

رابطه سرمایه روانشناختی و ارزیابی تهدید

اگرچه رفتارهای انگیزش حفاظت به‌طور سنتی بر ارزیابی تهدید تمرکز دارد، پژوهش‌های جدید نشان می‌دهند که سرمایه روان‌شناختی یکی از پیشایندهای مهم تقویت‌کننده این ارزیابی است. کارکنان بانکی که خودکارآمدی، امید و تاب‌آوری بیشتری دارند، در تحلیل موقعیت‌های پرخطر دقت بیشتری نشان می‌دهند و تهدیدات سایبری را جدی‌تر ارزیابی می‌کنند. مطالعه ژانگ و همکاران (۲۰۲۳) نشان داد که رابطه سرمایه روانشناختی و رفتار پیش‌نگرانه از طریق «ارزیابی ریسک / تهدید» میانجی‌گری می‌شود.

پیشینه پژوهش

1 Luthans & Youssef-Morgan

خلاصه پیشینه های تحقیق در جدول ۱ مشخص شده است.

جدول ۱. خلاصه پیشینه های پژوهش

نویسندگان	یافته اصلی	سال	عنوان فارسی	جامعه/حوزه	متغیرهای کلیدی
ریپتوئو و راجرز	ارزیابی‌های تهدید و مقابله، پاسخ‌های سازگارانه و ناسازگارانه را شکل می‌دهند.	۱۹۸۷	اثر مؤلفه‌های نظریه انگیزش حفاظت بر مقابله سازگارانه و ناسازگارانه با تهدید	حوزه سلامت	نظریه انگیزش حفاظت، ارزیابی تهدید، ارزیابی مقابله، ترس
حجت‌خواه، زکی‌یی و علیخانی	تاب‌آوری با فرسودگی رابطه معکوس دارد.	۱۳۹۱	رابطه تاب‌آوری و سلامت سازمانی با فرسودگی شغلی	معلمان	تاب‌آوری، سلامت سازمانی، فرسودگی شغلی
پوزی و همکاران	چارچوبی برای رفتارهای حفاظتی و انگیزشی ارائه می‌شود.	۲۰۱۳	حفاظت کارکنان داخلی از دارایی‌های اطلاعاتی سازمان: توسعه یک رده‌بندی سیستم‌محور و تبیین رفتارهای انگیزش حفاظت	سازمان‌ها	رفتارهای انگیزش حفاظت، دارایی اطلاعاتی، PMT
دمینو و بیمونت	SSM برای تحلیل ابعاد انسانی/سازمانی/فنی امنیت اطلاعات مناسب است.	۲۰۱۷	تحلیل امنیت اطلاعات در یک بانک با استفاده از روش‌شناسی سیستم‌های نرم	بانک	امنیت اطلاعات، روش‌شناسی سیستم‌های نرم
برنز و همکاران	سرمایه روان‌شناختی با ارزیابی تهدید/مقابله و انگیزه حفاظت پیوند دارد.	۲۰۱۷	بررسی رابطه سرمایه روان‌شناختی کارکنان داخلی با ارزیابی تهدید امنیت اطلاعات و ارزیابی‌های مقابله‌ای	کارکنان سازمان	سرمایه روان‌شناختی، ارزیابی تهدید، ارزیابی مقابله، انگیزه حفاظت
ورکمن، بامر و استراوب	ارزیابی تهدید/کنترل، رفتارهای امنیتی را پیش‌بینی می‌کند.	۲۰۰۸	لغزش‌های امنیتی و حذف اقدامات امنیت اطلاعات: مدل کنترل تهدید و آزمون تجربی	کاربران سیستم اطلاعاتی	کنترل تهدید، ارزیابی تهدید، پایبندی امنیتی
رحمان	ممیزی نشان‌دهنده ضعف و نیاز به بهبود است.	۲۰۱۶	ممیزی امنیت سیستم اطلاعات مدیریت بیمارستان بر اساس استاندارد ISO 27002:2005	بیمارستان	ISMS، ISO 27002
سوسانتو و شابریا	سطح پیاده‌سازی ISMS ارزیابی شد.	۲۰۱۶	ارزیابی سیستم مدیریت امنیت اطلاعات بر پایه استاندارد ISO/IEC 27001:2013	سازمان/شهرداری	ISMS، ISO 27001
رفیعی و همکاران	رفتار ایمنی در پیاده‌سازی موفق امنیت اطلاعات اثرگذار است.	۱۳۹۶	تأثیر رفتار ایمنی کارکنان بر پیاده‌سازی موفق امنیت اطلاعات در مدیریت دانش با نقش ویژگی‌های سازمانی	پژوهشگاه	رفتار ایمنی، امنیت اطلاعات، ویژگی‌های سازمانی

شیخی‌فر و همکاران	مدیریت منابع انسانی در استقرار امنیت اطلاعات نقش کلیدی دارد.	۱۳۹۶	نقش مدیریت منابع انسانی در شفافیت امور اداری و امنیت اطلاعات سازمان	سازمان	مدیریت منابع انسانی، شفافیت، امنیت اطلاعات
اسفندیارپور و اکبری	چند الگوی ذهنی برای رعایت سیاست‌های امنیتی شناسایی شد.	۱۳۹۵	شناسایی الگوهای ذهنی کارمندان درباره سیاست‌های امنیت اطلاعات	کارکنان	الگوهای ذهنی، سیاست‌های امنیت
حضرتی و عرفانیان‌خان‌زاده	امید به‌عنوان منبع روانی نقش میانجی دارد.	۱۳۹۵	نقش میانجی امید کارکنان در رابطه رهبری معتبر و خلاقیت کارکنان	کارکنان	امید، رهبری، خلاقیت
پیکری و بنازاده		۱۳۹۷	رابطه آگاهی از امنیت اطلاعات با قصد نقض امنیت اطلاعات با نقش میانجی هنجارهای فردی و خودکنترلی		آگاهی امنیتی، هنجار فردی، خودکنترلی، قصد نقض
عیدی و فروغی	افزایش آگاهی، افشای اطلاعات شخصی را کاهش می‌دهد.	۱۳۹۷	بررسی تأثیر تهدیدات امنیت اطلاعات بر افشای اطلاعات شخصی	کاربران اینترنت	تهدیدات امنیت اطلاعات، افشای اطلاعات
ترچانی نارنج‌بن، رضایی و بشکوه	ادراک تهدید ↑ انگیزه حفاظت ↑؛ ترس ↑ انگیزه حفاظت ↓	۱۴۰۳	تبیین ارتباط میان ارزیابی تهدید امنیت، ترس و انگیزه حفاظت از سیستم‌های اطلاعاتی حسابداری: آزمون نظریه روانشناسی مثبت‌گرا	حسابداران و مدیران مالی	ارزیابی تهدید، ترس، انگیزه حفاظت

در این پژوهش، با تکیه بر نظریه انگیزش حفاظت، نقش سرمایه روان‌شناختی کارکنان در تبیین انگیزه حفاظت از امنیت اطلاعات مورد بررسی قرار گرفته است. سرمایه روان‌شناختی به عنوان مجموعه‌ای از منابع روانی مثبت شامل خودکارآمدی، امیدواری، تاب‌آوری و خوش‌بینی در نظر گرفته می‌شود که می‌تواند نگرش‌ها و رفتارهای کارکنان را در محیط کار تحت تأثیر قرار دهد. از سوی دیگر، ارزیابی تهدید به عنوان یکی از مؤلفه‌های اصلی نظریه انگیزش حفاظت، بیانگر ادراک فرد از میزان جدی بودن تهدیدها و احتمال وقوع آن‌ها است و می‌تواند نقش مهمی در شکل‌گیری رفتارهای محافظتی ایفا کند. بر این اساس، در مدل مفهومی پژوهش حاضر، سرمایه روان‌شناختی به عنوان متغیر مستقل، انگیزه حفاظت از امنیت اطلاعات به عنوان متغیر وابسته و ارزیابی تهدید به عنوان متغیر میانجی در نظر گرفته شده است. انتظار می‌رود کارکنانی که از سطح بالاتری از سرمایه روان‌شناختی برخوردار هستند، تهدیدهای امنیت اطلاعات را جدی‌تر ارزیابی کرده و در نتیجه انگیزه بیشتری برای رعایت و حفاظت از امنیت اطلاعات سازمان داشته باشند.با توجه به چارچوب نظری پژوهش، فرضیه‌های زیر تدوین شده‌اند:

فرضیه اول: سرمایه روان‌شناختی کارکنان بر انگیزه حفاظت از امنیت اطلاعات تأثیر معنادار دارد.

فرضیه دوم: سرمایه روان‌شناختی کارکنان بر ارزیابی تهدید تأثیر معنادار دارد.

فرضیه سوم: ارزیابی تهدید بر انگیزه حفاظت از امنیت اطلاعات تأثیر معنادار دارد.

فرضیه چهارم: سرمایه روان‌شناختی کارکنان از طریق ارزیابی تهدید بر انگیزه حفاظت از امنیت اطلاعات تأثیر غیرمستقیم و معنادار دارد.

روش شناسی پژوهش

پژوهش حاضر از نظر هدف کاربردی و از نظر روش، توصیفی از نوع همبستگی است که با استفاده از مدل‌یابی معادلات ساختاری انجام شده است. جامعه آماری این پژوهش شامل کلیه کارکنان بانک ملی استان اصفهان به تعداد ۱۳۲۰ نفر بود. حجم نمونه بر اساس جدول کرجسی و مورگان تعیین شد و تعداد ۲۹۷ نفر به‌عنوان نمونه پژوهش انتخاب گردید.به منظور گردآوری داده‌ها از سه پرسشنامه استاندارد استفاده شد. برای سنجش سرمایه روان‌شناختی از پرسشنامه سرمایه روان‌شناختی لوتانز و همکاران (۲۰۰۷) استفاده گردید که ابعاد امیدواری، تاب‌آوری، خوش‌بینی و خودکارآمدی را اندازه‌گیری می‌کند. برای سنجش ارزیابی تهدید از پرسشنامه ارزیابی تهدید ورکمن و همکاران (۲۰۰۸) و برای سنجش انگیزه حفاظت از امنیت اطلاعات از پرسشنامه انگیزه حفاظت از امنیت اطلاعات پوزی و همکاران (۲۰۱۵) استفاده شد. روایی ابزارهای پژوهش از طریق روایی محتوا و سازه مورد بررسی قرار گرفت و پایایی آن‌ها با استفاده از ضریب آلفای کرونباخ تأیید شد. پس از جمع‌آوری داده‌ها، برای تجزیه و تحلیل داده‌ها از آمار توصیفی و استنباطی استفاده شد. در بخش آمار توصیفی از نرم‌افزار SPSS و برای آزمون مدل مفهومی پژوهش و بررسی روابط بین متغیرها از مدل‌یابی معادلات ساختاری با استفاده از نرم‌افزار SmartPLS بهره گرفته شد.

یافته‌های پژوهش

نتیجه تحلیل توصیفی متغیرهای پژوهش در جدول ۲ نشان داده شده است. در جدول، برای هر یک از متغیرهای پژوهش و ابعاد آنها، آمار توصیفی شامل میانگین و انحراف استاندارد بیان شده است.

جدول ۲. میانگین و انحراف معیار متغیرهای اصلی پژوهش و ابعاد آن‌ها

متغیر	میانگین	انحراف معیار
۳/۶۳۱سرمایه روان‌شناختی	۳/۶۳۱	۰/۵۱۸
امیدواری	۳/۴۶۹	—
تاب‌آوری	۳/۶۲۹	—
خوش‌بینی	۳/۷۹۱	—
خودکارآمدی	۳/۶۶۷	—
ارزیابی تهدید	۳/۳۶۱	۰/۶۲۷
شدت تهدید	۲/۲۳۸	—
ارزیابی پاداش	۲/۴۲۳	—

۰/۶۵۴	۳/۵۸٦	انگیزه حفاظت از امنیت اطلاعات

بر اساس نتایج جدول ۱، میانگین سرمایه روان‌شناختی (۳/۶۳۱) و انگیزه حفاظت از امنیت اطلاعات (۳/۵۸۶)(۳/۵۸۶)(۳/۵۸۶) بالاتر از حد متوسط است که نشان می‌دهد کارکنان از سطح نسبتاً مطلوبی در این دو متغیر برخوردار بوده‌اند. در مقابل، میانگین ارزیابی تهدید (۲/۳۶۱) پایین‌تر از حد متوسط به دست آمد. همچنین در بین ابعاد سرمایه روان‌شناختی، خوش‌بینی با میانگین ۳/۷۹۱بیشترین مقدار را به خود اختصاص داد.سرمایه روان‌شناختی: میانگین (۳/۶۳۱) و انحراف معیار (۰/۵۱۸)؛ بالاتر از حد متوسط. امیدواری (۳/۴۶۹)، تاب‌آوری (۳/۶۲۹)، خوش‌بینی (۳/۷۹۱) و خودکارآمدی (۳/۶۶۷). ارزیابی تهدید اطلاعات میانگین (۳/۴۲) و انحراف معیار (۰/۵۹۸)؛ بیانگر شناخت و حساسیت مطلوب کارکنان نسبت به امنیت اطلاعات است.انگیزه حفاظت از امنیت اطلاعات: میانگین (۳/۵۸۶) و انحراف معیار (۰/۶۵۴)؛ در سطح نسبتاً بالا قرار دارد.به‌طور کلی، داده‌ها از توزیع مناسب برخوردار بوده و برای مدل‌یابی معادلات ساختاری قابل استفاده‌اند.

پایایی و روایی سازه‌ها طبق جدول ۳ با استفاده از شاخص‌های AVE، CR و آلفای کرونباخ ارزیابی گردید. همه مقادیر CR بالاتر از ۰/۷ و AVE بالاتر از ۰/۵ به دست آمدند که نشان‌دهنده‌ی روایی همگرا و پایایی مطلوب هستند.

جدول ۳. محاسبه روایی و پایایی ابزار سنجش

نتیجه	آلفای کرونباخ	CR	AVE	سازه
مطلوب	۰/۸۵۰	۰/۸۹۱	۰/۵۶۸	سرمایه روان‌شناختی
مطلوب	۰/۸۴۱	۰/۸۵۴	۰/۵۴۲	ارزیابی تهدیداطلاعات
مطلوب	۰/۸۶۹	۰/۸۷۷	۰/۶۳۱	انگیزه حفاظت

روایی واگرا نیز با معیار HTMT تأیید شده است (همه مقادیر < ۰/۸۵).

پس از تأیید مدل اندازه‌گیری، روابط میان سازه‌ها طبق جدول ۴ در مدل ساختاری تحلیل شد.

جدول ٤. مدل ساختاری و آزمون فرضیه‌ها

نتیجه آماری	t-value	ضریبβ	مسیر
معنادار	۳/۱۲۶	۰/۸۹۵	سرمایه روان‌شناختی ← ارزیابی تهدیداطلاعات
معنادار	۲/۹۸۷	۰/۴۴۵	ارزیابی تهدید اطلاعات ← انگیزه حفاظت از امنیت اطلاعات
غیرمعنادار	۱/۶۳۲	۰/۲۳۹	سرمایه روان‌شناختی ← انگیزه حفاظت از امنیت اطلاعات

سرمایه روان‌شناختی اثر مثبت و معناداری بر ارزیابی تهدید اطلاعات دارد. همچنین ارزیابی تهدید اطلاعات پیش‌بینی‌کننده‌ی معنادار انگیزه حفاظت است. با این‌حال، اثر مستقیم سرمایه روان‌شناختی بر انگیزه حفاظت

شاخص‌های برازش مدل: برازش کلی مدل بر اساس شاخص‌های استاندارد جدول ۵ تأیید شد.

جدول ۵. برازش کلی مدل

نتیجه	معیار توصیه‌شده	مقدار	شاخص برازش
مطلوب	۰/۰۸ >	۰/۰۶۷	SRMR
مطلوب	۰/۹۰ <	۰/۹۱	NFI
مطلوب	۰/۱۲ >	۰/۱۰	RMS Theta
برازش کلی مناسب	۰/۴۰ <	۰/۴۸	GoF

این مقادیر نشان‌دهنده تطابق مناسب مدل با داده‌های تجربی و کفایت ساختار نظری پژوهش است.

همچنین جدول ۶ ضرایب مسیر مستقیم بین متغیرهای پژوهش را نشان می دهد.

جدول ٦. ضرایب مسیر مستقیم بین متغیرهای پژوهش

نتیجه	آماره تی	ضریب مسیر	مسیر
غیرمعنادار	۱/۶۳۲	۰/۲۳۹	سرمایه روان‌شناختی ← انگیزه حفاظت از امنیت اطلاعات
معنادار	۴۵/۷۸۶	۰/۸۹۵	سرمایه روان‌شناختی ← ارزیابی تهدید
معنادار	۳/۱۳۴	۰/۴۴۵	ارزیابی تهدید ← انگیزه حفاظت از امنیت اطلاعات

نتایج جدول ۶ نشان داد مسیر سرمایه روان‌شناختی به ارزیابی تهدید با ضریب ۰/۸۹۵ معنادار است. همچنین مسیر ارزیابی تهدید به انگیزه حفاظت از امنیت اطلاعات با ضریب ۰/۴۴۵ معنادار گزارش شد. با این حال، اثر مستقیم سرمایه روان‌شناختی بر انگیزه حفاظت از امنیت اطلاعات با ضریب ۰/۲۳۹ غیرمعنادار شد.

جدول ۷ نیز اثر غیرمستقیم و میانجی‌گری ارزیابی تهدید در رابطه بین سرمایه روان‌شناختی و انگیزه حفاظت از امنیت اطلاعات را نشان می دهد.

جدول ۷. اثر غیرمستقیم و میانجی‌گری ارزیابی تهدید در رابطه بین سرمایه روان‌شناختی و انگیزه حفاظت از امنیت اطلاعات

نتیجه	VAF مقدار	Z آماره	مسیر غیرمستقیم
میانجی‌گری نسبی و معنادار	۰/۶۱۱	۳/۱۲۶	سرمایه روان‌شناختی ← ارزیابی تهدید ← انگیزه حفاظت از امنیت اطلاعات

نتایج آزمون میانجی‌گری طبق جدول ۷ نشان داد اثر غیرمستقیم سرمایه روان‌شناختی بر انگیزه حفاظت از امنیت اطلاعات از طریق ارزیابی تهدید معنی‌دار است. مقدار شاخص بیانگر آن است که حدود ۶۱ درصد از کل اثر سرمایه روان‌شناختی بر انگیزه حفاظت از مسیر میانجی ارزیابی تهدید منتقل می‌شود. این یافته نشان‌دهنده میانجی‌گری نسبی ارزیابی تهدید است؛ بدین معنا که ارزیابی تهدید نقش مهمی در تبیین ارتباط سرمایه روان‌شناختی و انگیزه رفتارهای حفاظتی ایفا می‌کند. شاخص های روایی همگرا و پایایی ترکیبی سازه ها طبق جدول ۸ مشخص شده اند.

جدول ۸. شاخص‌های روایی همگرا و پایایی ترکیبی سازه‌ها

سازه	AVE (میانگین واریانس استخراج‌شده)	CR (پایایی ترکیبی)	نتیجه
سرمایه روان‌شناختی	کمتر از ۰/۵۰	مطلوب	پایایی مناسب، اما روایی همگرا ضعیف
ارزیابی تهدید	مناسب	مطلوب	روایی و پایایی قابل قبول
انگیزه حفاظت از امنیت اطلاعات	مناسب	مطلوب	روایی و پایایی قابل اعتماد

شاخص‌های روایی و پایایی نشان دادند که تمام سازه‌ها از پایایی مطلوبی برخوردارند. اگرچه مقدار AVE برای سازه سرمایه روان‌شناختی کمتر از ۰/۵۰ بود (که بیانگر روایی همگرای کمتر از حد مطلوب است)، اما مقدار بالای CR نشان‌دهنده انسجام درونی و پایایی کافی مقیاس است. سازه‌های ارزیابی تهدید و انگیزه حفاظت نیز از نظر روایی همگرا و پایایی ترکیبی در وضعیت رضایت‌بخشی قرار دارند.

جدول ۹. شاخص‌های برازش مدل معادلات ساختاری

شاخص برازش	مقدار به‌دست‌آمده	تفسیر
SRMR	کمتر از ۰/۰۸	برازش مطلوب مدل
NFI	بیشتر از ۰/۹۰	تطابق مناسب
GoF	بیشتر از ۰/۴۰	کفایت کلی برازش
۲R^2R۲R انگیزه حفاظت	قابل قبول	مقدار تبیین مناسب واریانس متغیر درون‌زا

شاخص‌های برازش مدل بیانگر آن هستند که مدل مفهومی پژوهش از برازش مناسبی برخوردار است؛ مقدار SRMR کمتر از ۰/۰۸ و NFINFINFI بالاتر از ۰/۹۰ نشان‌دهنده مطلوب بودن برازش کلی مدل است. همچنین مقدار مناسب GoFGoFGoF و ۲R^2R۲R بیانگر آن است که مدل توانسته است بخش قابل توجهی از واریانس متغیرهای درون‌زا را تبیین کند. در نتیجه می‌توان گفت مدل معادلات ساختاری پژوهش از کفایت آماری و مفهومی کافی برخوردار است.

تمام مسیرهای اصلی مدل (به جز مسیر مستقیم سرمایه روان‌شناختی ← انگیزه حفاظت) از نظر آماری معنی‌دار بودند.مقدار بالای β=۰،۸۹۵ = β۰،۸۹۵=۰،۸۹۵ در مسیر سرمایه روان‌شناختی ← ارزیابی تهدید نشان می‌دهد کارکنان با سطح سرمایه روان‌شناختی بالاتر نسبت به تهدیدهای امنیتی حساس‌تر و هوشیارتر عمل می‌کنند.مسیر ارزیابی تهدید ← انگیزه حفاظت با ضریب ۰،۴۴۵ مؤید آن است که هرچه ادراک و تحلیل کارکنان از تهدیدهای امنیتی افزایش یابد، رفتارهای حفاظتی آنان نیز تقویت می‌گردد.شاخص میانجی‌گری VAF=۰،۶۱۱ نشان می‌دهد بخش عمده‌ای از اثر کل سرمایه روان‌شناختی بر انگیزه حفاظت از مسیر ارزیابی تهدید منتقل می‌شود.

نتیجه گیری

پژوهش حاضر با هدف تبیین نقش سرمایه روان‌شناختی در شکل‌گیری انگیزه حفاظت از امنیت اطلاعات با تأکید بر نقش میانجی ارزیابی تهدید در میان کارکنان بانک ملی استان اصفهان انجام شد. نتایج مدل‌یابی معادلات ساختاری نشان داد که سرمایه روان‌شناختی به‌طور معناداری ارزیابی تهدید کارکنان را تحت تأثیر قرار می‌دهد و ارزیابی تهدید نیز پیش‌بینی‌کننده معنادار انگیزه حفاظت از امنیت اطلاعات است. این یافته‌ها نشان می‌دهد کارکنانی که از سطح بالاتری از امید، تاب‌آوری، خوش‌بینی و خودکارآمدی برخوردارند، توانایی بیشتری در تشخیص و ارزیابی تهدیدهای امنیتی داشته و در نتیجه انگیزه بیشتری برای رعایت رفتارهای حفاظتی در محیط سازمانی از خود نشان می‌دهند.

یافته‌های پژوهش همچنین نشان داد که اثر مستقیم سرمایه روان‌شناختی بر انگیزه حفاظت از امنیت اطلاعات معنادار نیست، اما اثر غیرمستقیم آن از طریق ارزیابی تهدید معنادار و قابل توجه است. مقدار شاخص VAF برابر با ۰.۶۱۱ نشان می‌دهد که بخش قابل توجهی از اثر سرمایه روان‌شناختی بر انگیزه حفاظت از طریق سازوکار شناختی ارزیابی تهدید منتقل می‌شود. این نتیجه بیانگر آن است که منابع روان‌شناختی مثبت کارکنان ابتدا بر نحوه ادراک آنان از تهدیدهای امنیتی اثر می‌گذارند و سپس از این مسیر انگیزه لازم برای رفتارهای محافظتی شکل می‌گیرد. از منظر نظری، یافته‌های این پژوهش به گسترش ادبیات نظریه انگیزش حفاظت در حوزه امنیت اطلاعات کمک می‌کند. در حالی که این نظریه عمدتاً بر فرآیندهای شناختی ارزیابی تهدید و ارزیابی مقابله تمرکز دارد، نتایج پژوهش حاضر نشان می‌دهد که سرمایه روان‌شناختی به‌عنوان یک منبع روانی مثبت می‌تواند به‌عنوان پیشایند مهمی در شکل‌گیری این ارزیابی‌ها نقش‌آفرینی کند. بنابراین، ترکیب مفاهیم روان‌شناسی مثبت با نظریه انگیزش حفاظت می‌تواند چارچوب جامع‌تری برای تبیین رفتارهای امنیت اطلاعات در سازمان‌ها فراهم آورد.

از منظر کاربردی، نتایج این پژوهش نشان می‌دهد که ارتقای امنیت اطلاعات در سازمان‌های بانکی صرفاً از طریق ابزارهای فناورانه یا سیاست‌های کنترلی امکان‌پذیر نیست و توجه به ابعاد انسانی و روان‌شناختی کارکنان نیز ضروری است. تقویت سرمایه روان‌شناختی کارکنان از طریق برنامه‌های آموزشی، کارگاه‌های توسعه فردی، آموزش تاب‌آوری سازمانی و ارتقای

خودکارآمدی می‌تواند حساسیت کارکنان نسبت به تهدیدهای امنیت اطلاعات را افزایش داده و در نهایت رفتارهای حفاظتی آنان را تقویت کند. همچنین طراحی برنامه‌های آموزشی هدفمند در حوزه آگاهی‌بخشی امنیت اطلاعات می‌تواند فرآیند ارزیابی تهدید را در میان کارکنان تقویت کرده و به ارتقای فرهنگ امنیت اطلاعات در سازمان‌های مالی کمک نماید.

در تبیین این یافته، می‌توان گفت که کارکنان با سرمایه روان‌شناختی بالا (امید، تاب‌آوری، خوش‌بینی و خودکارآمدی)، در مواجهه با تهدیدات، رویکردی منفعل ندارند. چنان‌که دانلان (۲۰۲۳) اشاره می‌کند، مدیریت و رهبری مؤثر نقشی حیاتی در بهبود عملکرد سازمانی دارد؛ در اینجا نیز منابع روانی مثبت، مانند یک "رهبری درونی" عمل کرده و موجب می‌شوند فرد تهدید را دقیق‌تر ارزیابی کند. این سازوکار شناختی با مفهوم «بینش کلان» که توسط هاجیومروویچ (۲۰۲۱) به عنوان یکی از ابعاد شرافت مدیریتی مطرح شده، قرابت دارد؛ چرا که فرد با بینشِ برآمده از سرمایه روان‌شناختی، پیامدهایِ بی‌توجهی به امنیت را عمیق‌تر درک می‌کند.

یافته دیگر مبنی بر عدم اثر مستقیم سرمایه روان‌شناختی بر انگیزه حفاظت، اما معناداری اثر غیرمستقیم آن، بیانگر نقش کلیدیِ «ارزیابی تهدید» به عنوان یک میانجی شناختی است. در واقع، سرمایه روان‌شناختی به تنهایی برای ایجاد انگیزه حفاظت کافی نیست، بلکه باید در قالبِ درکِ خطر (ارزیابی تهدید) متبلور شود. این یافته با مبانی نظری قلی‌پور (۱۴۰۳) در مورد تمایز رهبری اخلاقی و چهبری، قابل تفسیر است؛ به‌گونه‌ای که سرمایه روان‌شناختی با تقویت نگاه اخلاقی به وظایف شغلی، فرد را نسبت به حفظ امنیت (به‌عنوان یک وظیفه در قبال سازمان) حساس‌تر می‌کند.

از منظر کاربردی، این پژوهش پیشنهاد می‌کند که امنیت اطلاعات صرفاً یک موضوع فنی نیست. با الهام از چارچوب چترجی و همکاران (۲۰۲۱) که پیوند شفقت با فناوری اطلاعات را پیشنهاد داده‌اند، می‌توان گفت در سازمان‌های بانکی نیز باید پیوند میان «منابع انسانی مثبت» و «زیرساخت‌های فنی» برقرار شود. همچنین، با توجه به دیدگاه پاکانن و همکاران (۲۰۲۰) مبنی بر آموختنی بودن مهارت‌های احساسی، پیشنهاد می‌شود سازمان‌های بانکی با برگزاری کارگاه‌های توسعه سرمایه روان‌شناختی، نه تنها تاب‌آوری کارکنان را افزایش دهند، بلکه حساسیت آنان نسبت به مقوله امنیت را نهادینه کنند. این امر در راستای یافته‌های دهقانی‌زاده (۱۴۰۳) در مورد شرافت کاری است؛ چرا که رعایت الزامات امنیتی، جلوه‌ای از اخلاق حرفه‌ای و شرافت کاری کارمند نسبت به ذی‌نفعان بانک محسوب می‌شود.

در نهایت، با توجه به محدودیت‌های پژوهش و تأکید الشعلان و گومروم (۲۰۲۲) بر تفاوت‌های فرهنگی در هنجارهای اخلاقی، پیشنهاد می‌شود در پژوهش‌های آتی، نقش فرهنگ سازمانی و متغیرهای اخلاقی-محیطی که در مطالعات دهقانی‌زاده و بابای‌زاده (۱۴۰۱) به عنوان پیشایندهای شرافت کاری مطرح شده‌اند، در مدل‌های توسعه‌یافته مورد آزمون قرار گیرند تا دیدگاه جامع‌تری نسبت به رفتارهای امنیت اطلاعات فراهم شود. با وجود نتایج ارزشمند، این پژوهش دارای محدودیت‌هایی نیز بود. تمرکز پژوهش بر کارکنان یک بانک و استفاده از داده‌های خودگزارشی می‌تواند تعمیم‌پذیری نتایج را محدود کند. بنابراین پیشنهاد می‌شود پژوهش‌های آینده این مدل را در سایر سازمان‌های مالی و خدماتی مورد

آزمون قرار دهند و متغیرهای دیگری مانند فرهنگ امنیت اطلاعات، رهبری سازمانی و آگاهی امنیتی را نیز در مدل‌های پژوهشی وارد کنند.

در مجموع، نتایج این پژوهش نشان می‌دهد که سرمایه روان‌شناختی از طریق تقویت ارزیابی تهدید می‌تواند نقش مهمی در افزایش انگیزه حفاظت از امنیت اطلاعات در میان کارکنان ایفا کند. توجه هم‌زمان به توسعه منابع روان‌شناختی کارکنان و ارتقای آگاهی امنیتی می‌تواند راهبردی مؤثر برای کاهش آسیب‌پذیری‌های انسانی و تقویت امنیت اطلاعات در سازمان‌های بانکی باشد. پژوهش حاضر با هدف تبیین نقش سرمایه روان‌شناختی در انگیزه حفاظت از امنیت اطلاعات با تأکید بر نقش میانجی ارزیابی تهدید انجام شد. یافته‌ها نشان داد که سرمایه روان‌شناختی از طریق ارزیابی تهدید، انگیزه حفاظت را تحت تأثیر قرار می‌دهد. این یافته با مطالعاتی که بر نقش منابع درونی در فرآیندهای شناختی تأکید دارند، همسو است.

ملاحظات اخلاقی

مشارکت نویسندگان

مفهوم‌سازی: علیرضا گلی ؛ روش‌شناسی و تحلیل رسمی: حمیدرضا پیکری ؛ نگارش پیش‌نویس اصلی: علیرضا گلی؛ نگارش – بررسی و ویرایش: همه نویسندگان؛ نظارت: حمیدرضا پیکری.

تقدیر و تشکر

نویسندگان هیچ بودجه خاصی برای این کار دریافت نکرده‌اند. از داوران ناشناس به خاطر نظرات بخردانه‌شان سپاسگزاریم.

تعارض منافع

نویسندگان هیچ تضاد منافعی را اعلام نکردند.

یادداشت ناشر

ناشر در مورد ادعاهای مربوط به صلاحیت در نقشه‌های منتشر شده و وابستگی‌های نهادی بی‌طرف می‌ماند.

بیانیه مثبت هوش مصنوعی

ابزارهای هوش مصنوعی ((AI، از جمله مدل‌های زبانی بزرگ، صرفاً برای ویرایش زبان و بهبود خوانایی در این نسخه خطی استفاده شده‌اند. هوش مصنوعی برای تولید ایده، تجزیه و تحلیل داده‌ها، تفسیر نتایج یا نوشتن محتوای علمی استفاده نشده است. تمام مشارکت‌های فکری و تصمیمات علمی توسط نویسندگان انسانی گرفته شده است.

اختصارات

PsyCap = سرمایه روانشناختی PM = انگیزه محافظت PMT = نظریه انگیزه محافظت IS / InfoSec= امنیت اطلاعات

نویسنده(گان) طرح‌های زیستی

حمیدرضا پیکری، استادیار گروه علوم ارتباطات و کسب‌وکار در دانشگاه آزاد اسلامی واحد اصفهان (خوراسگان)، اصفهان، ایران است. وی همچنین به عنوان عضو هیأت تحریریه نشریه تحقیقات علوم داده‌های کسب‌وکار فعالیت دارد. حوزه‌های پژوهشی مورد علاقه ایشان شامل رفتار سازمانی و توسعه کسب‌وکار است. نویسنده مسئول: ایمیل: omid726@yahoo.com

References

Akhlaqi, H. (2016). Foundations and behavioral patterns of desirable lifestyle from the perspective of the Holy Quran (Master's thesis). Supervisor: Seyed Hossein Sharafeddin, Al-Mustafa International University, Islamic Sciences Research Center. [In Persian]

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

Anwar, M., He, W., & Ash, I. (2020). Information security policy compliance: A comprehensive meta-analysis. *Computers & Security*, 92, 101748. DOI: 10.1016/j.cose.2020.101748

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. Computers in Human Behavior, 68, 190–209. DOI: 10.1016/j.chb.2016.11.018

Damenu, T. K., & Beaumont, C. (2017). Analysing information security in a bank using soft systems methodology. Information & Computer Security, 25(3), 240–258. DOI: 10.1108/ICS-07-2016-0053

Dehghani, M., Rahmatpasand-Fatideh, Z., Arasteh, Z., & Shokrizadeh-Bezenjani, K. (2019). Awareness, attitude, and performance of health information management staff in Iranian hospitals regarding health information security. *Health Information Management*, 16(1), 3–9 [In Persian]. https://doi.org/10.22122/him.v16i1.3727

Esfandiarpour, R., & Akbari, M. (2016). Identifying employees' mental models regarding information security policies. *Journal of Information Technology Management*, 8(2), 215–230 [In Persian].

Eydi, F., & Foroughi, S. (2018). Investigating the impact of information security threats on personal information disclosure (Case study: Internet users at Payame Noor University of Alborz). *Proceedings of the Third National Conference on Technology in Electrical and Computer Engineering*, Semnan, Payame Noor University. [In Persian]. https://civilica.com/doc/1795999

Firozbakhsh, M.; Eidi F. and Yousefi Pour M., (2016), "Examining the Relationship between Internal Employees' Psychology and Information Security Threats and Assessing Threat Response," *First National Conference on Information and Communication Technology Advances and Opportunitie*s, Tehran, Cultural Studies University.

Hazrati, Q., & Erfanian-Khanzadeh, H. (2016). Investigating the mediating role of employees' hope in the relationship between authentic leadership and employee creativity. *Proceedings of the Comprehensive Conference on Management and Accounting Sciences*, Tehran, Secretariat of the Comprehensive Conference on Management and Accounting Sciences [In Persian].

Hojatkhah, M., Zakiyi, A., & Alikhani, M. (2012). The relationship between resilience and organizational health with job burnout among female elementary school teachers in Kermanshah. *Cognitive Analytical Psychology*, 35–44 [In Persian].

Ifinedo, P. (2019). Understanding information security policy compliance: An integration of the theory of planned behavior and protection motivation theory. *Computers & Security*, 83, 375–389. DOI: 10.1016/j.cose.2019.02.009

Kim, J., & Koeske, S. (2022). The influence of psychological capital on cybersecurity compliance behavior. Cyberpsychology, *Behavior, and Social Networking*, 25(8), 493–501. DOI: 10.1089/cyber.2021.0432

Luthans, F., & Youssef-Morgan, C. (2022). Psychological Capital and Beyond: Developing human strengths in organizations. *Oxford University Press*.

Luthans, F., Youssef, C. M., & Avolio, B. J. (2007b). Psychological Capital: Developing the human competitive edge. *New York, NY: Oxford University Press*.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469-479.

Parker, S. K. (1998). Enhancing role breadth self-efficacy: The roles of job enrichment and other organizational interventions. *Journal of Applied Psychology*, 83(6), 835-852. DOI:10.1037//0021-9010.83.6.835

Pikri, H., & Banazadeh, B. (2018). The relationship between information security awareness and intention to violate information security with the mediating role of personal norms and self-control. *Strategic Research on Social Issues*, 7(4), 41–58 [In Persian]. https://doi.org/10.22108/ssoss.2019.108446.1174

Posey, C., Lowry, P. B., & Roberts, T. L. (2021**).**The protection motivation theory in organizational security behavior: A meta-analytic review.*Information Systems Research, 32(4),* 987–1003. DOI: 10.1287/isre.2021.1041

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders'protection of organizational information assets: Development of a systematicsbasedtaxonomy and theory of diversity for protection-motivated behaviors.*MIS quarterly*, 37(4), 1189-1210. DOI:10.25300/MISQ/2013/37.4.09

Rafiei, S., Hassani, M., & Abtahi, A. (2017). Measuring the impact of employees' safety behavior on successful implementation of information security in organizational knowledge management considering organizational characteristics: A case study of the ICT Research Institute. *Proceedings of the Second International Conference on Management and Accounting*, Tehran, Salehan Higher Education Institute. [In Persian]. https://civilica.com/doc/492563

Rahman, A. N. (2016). TA: Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Berdasarkan ISO 27002: 2005 Pada Rumah Sakit Islam Jemursari (Doctoral dissertation, Institut Bisnis dan Informatika Stikom Surabaya). http://repository.dinamika.ac.id/id/eprint/2103

Rahman, A. N. (2016). TA: Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Berdasarkan ISO 27002: 2005 Pada Rumah Sakit Islam Jemursari (Doctoral dissertation, Institut Bisnis dan Informatika Stikom Surabaya). https://repository.dinamika.ac.id/id/eprint/2103/1/COVER.pdf

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protectionmotivationtheory on adaptive and maladaptive coping with a health threat.Journal of Personality and Social Psychology, 52(3), 596-604. https://doi.org/10.1037/0022-3514.52.3.596

Sheikhifar, R., Kooknar, J., & Khosravani, A. (2017). Investigating the role of human resource management in administrative transparency and organizational information security: A case study of the General Directorate of Arak Railway. *Proceedings of the Sixth National Conference on Modern Management Sciences*, Gorgan, Golestan Association of Professional Managers and Accountants. [In Persian].

Sheldon, K. M., & King, L. (2001). Why positive psychology is necessary. *American Psychologist*, 56(3), 216-217. DOI:10.1037/0003-066X.56.3.216

Shobariah, E. (2016, April). Assessment of ISMS based on standard ISO/IEC 27001:2013 at DISKOMINFO Depok City. In Cyber and IT Service Management, International Conference on (pp. 1–6). IEEE. DOI: 10.1109/CITSM.2016.7577471

Susanto, A., &Cisco. (2013). Cisco annual security report. Retrieved from http://www.cisco . com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf.

Tarchani Narenjbon, A., Rezaei, F., & Beshkouh, M. (2024). Explaining the relationship between security threat appraisal, fear, and motivation to protect accounting information systems: Testing positive psychology theory. *Journal of Management Accounting and Auditing Knowledge*, 15(58), 537–547. https://doi.org/10.22034/jmaak.2025.78109.4440 [Persian]

Vance, A., Lowry, P. B., & Eggett, D. (2015). A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface. *MIS Quarterly*, 39(2), 345-366. https://www.researchgate.net/publication/270813385_A_new_approach_to_the_problem_of_access_policy_violations_Increasing_perceptions_of_accountability_through_the_user_interface

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), 2799–2816. 10.1016/j.chb.2008.04.005

Zhang, L., Guo, Y., & Yan, X. (2023). Psychological capital and proactive organizational behavior: The mediating role of risk appraisal. *Journal of Occupational Psychology*, 52(4), 377–394. DOI: 10.1111/joop.12456

Zhao, H., Wen, X., & Zhang, W. (2025).Psychological capital and risk perception in digital workplaces.*Computers in Human Behavior, 147,* 107950.DOI: 10.1016/j.chb.2024.107950