Iranian Journal of Ergonomics

Iran J Ergon, 2026; 13(4): 307-317 DOI:10.53208/IJE.13.4.307

https://journal.iehfs.ir/

Original Article

A Model Based on Macro-ergonomics to Improve Cybersecurity Resilience and Reduce Financial Risk in Digital Banking: A Mixed-Method Study

Nabi Omidi[1], Hasan Ghanbarzadeh[2], Mohsen Emami[3], Mohammadreza Omidi[4*]

[1] Department of Management, Payame Noor University, Tehran, Iran
[2] Department of Information Technology Management, Islamic Azad University, South Tehran Branch, Tehran, Iran
[3] Department of Information Technology Management, Islamic Azad University, Science and Research Branch, Tehran, Iran
[4] Department of Industrial Engineering, Payame Noor University, Tehran, Iran

Article History:
Received: 30 September 2025
Revised: 15 January 2026
Accepted: 16 January 2026
ePublished: 20 March 2026

***Corresponding author:**
Mohammadreza Omidi, Department of Industrial Engineering, Payame Noor University, Tehran, Iran

Email: mromidi_91@yahoo.com

Abstract

Objectives: With the increasing expansion of digital banking, cyber threats have become a significant financial and operational risk. This study aimed to develop a model grounded in macro-ergonomic principles to enhance cybersecurity resilience and reduce financial risk in the digital banking industry.

Methods: This study used a mixed-methods approach. In the qualitative phase, 15 experts were interviewed, and the data were examined using thematic analysis. In the quantitative phase, the resulting conceptual model was tested using a researcher-developed questionnaire administered to 387 bank employees. Data analysis and final model evaluation were performed using structural equation modeling (SEM) in LISREL software.

Results: The qualitative analysis identified five main themes and 32 sub-themes that formed the dimensions of the model: technical-instrumental subsystem, human-psychological, organizational-structural, environmental-supervisory factors, and cybersecurity resilience (consequence). The results of the quantitative model test showed that the model had a good fit (minimum discrepancy function by degrees of freedom divided [CMIN/DF] = 2.41, goodness of fit index [GFI] = 0.92, comparative fit index [CFI] = 0.94, root mean square error of approximation [RMSEA] = 0.061, standardized root mean square [SRMR] = 0.057). All four macro-ergonomic dimensions had a positive and significant effect on cybersecurity resilience. Among them, the "organizational-structural subsystem" with a standardized path coefficient of 0.48 had the most critical impact and was identified as the strongest predictor.

Conclusion: The sociotechnical model based on macroergonomics provides an efficient framework for analyzing and strengthening cybersecurity resilience in digital banking, thereby helping reduce financial risks. This result emphasizes the need to transition from purely technical approaches to a systemic, interactive approach among humans, technology, and organizational structures.

Keywords: Cybersecurity, Digital banking, Macro-ergonomics, Resilience, Sociotechnical approach

Extended Abstract

Background and Objective

Rapid technological advancements have made digital banking one of the most vulnerable sectors to cyber threats. Focusing solely on technical infrastructure is insufficient, as human, organizational, and cultural factors also play a pivotal role in system resilience. Macro-ergonomics, with its systemic perspective, integrates human, technological, and structural interactions within socio-technical frameworks. From an economic perspective, weak cybersecurity resilience increases financial risk and undermines public trust. Given the limited attention paid by previous studies to integrative approaches, this research aimed to develop a socio-technical model based on macro-ergonomics using a mixed-methods design (qualitative–quantitative) and structural equation modeling (SEM) to provide a comprehensive framework for strengthening cybersecurity and reducing financial risk in Iran's digital banking.

Materials and Methods

This study employed a mixed-methods design with a sequential exploratory approach. In the first phase, the qualitative sector identified socio-technical dimensions influencing cybersecurity resilience in digital banking. The qualitative population included academic experts and industry professionals in ergonomics, information security, technology management, and the Iranian banking system. Purposeful and snowball sampling were performed until theoretical saturation was achieved, which occurred after 15 semi-structured interviews. Data were collected through open-ended questions regarding human–technology interaction, structural and cultural challenges in implementing security policies, and experiences with cyber incidents. Qualitative data were analyzed using Braun and Clarke's thematic analysis approach in MAXQDA version 2020, and five main themes and 32 subthemes were identified.

In the second phase, the quantitative sector was conducted to test the conceptual model. The statistical population consisted of employees and managers working in digital banking units of several selected Iranian banks in 2024. Power analysis ($\alpha = 0.05$, power = 0.99) indicated a sample size of 387 participants, and proportional stratified random sampling was used. The research instrument was a five-variable questionnaire developed from the qualitative phase results, finalized after a ten-member expert panel confirmed content validity and a pilot study involving 30 participants. Quantitative data were analyzed using LISREL and SPSS. The measurement model was first tested using confirmatory factor analysis (CFA), and satisfactory fit indices were reported. Subsequently, the structural model was examined using structural equation modeling (SEM) to identify relationships among the technical, human, organizational, and environmental subsystems and resilience and financial risk reduction. All analyses were conducted at a significance level of less than 0.05.

Results

Quantitative data analysis revealed that the socio-technical model based on macro-ergonomics demonstrated satisfactory statistical fitness, and the relationships among subsystems were significantly confirmed. The confirmatory factor analysis (CFA) results indicated adequate factor loadings and construct validity. Furthermore, the structural model tested in LISREL indicated acceptable goodness-of-fit indices. The findings showed that the organizational–structural subsystem was the strongest predictor of cybersecurity resilience ($\beta = 0.47$), followed by the human–psychological ($\beta = 0.32$), technical–instrumental ($\beta = 0.29$), and environmental–regulatory subsystems ($\beta = 0.21$). The indirect effects of the human and technical subsystems were also observed through structural coordination and enhancement of internal communication. Overall, the model explained more than 65% of the variance in resilience, confirming that cybersecurity resilience in banks results from the systematic interaction among human, structural, technological, and environmental factors rather than from merely improving technical infrastructure.

Discussion

The results of this study indicate that enhancing cybersecurity resilience in digital banking cannot be achieved solely by improving technical infrastructure but rather through the comprehensive interaction of human, organizational, technical, and environmental elements. The organizational–structural subsystem emerged as the most influential factor affecting cybersecurity resilience, underscoring the critical role of organizational culture, cross-departmental coordination, decision-making mechanisms, and internal communication in financial cyber defense. This suggests that flexible and participatory organizational structures strengthen banks' capacity to adapt and respond effectively to emerging digital threats. The significant influence of the human–psychological subsystem highlights that employees' competence, trust, motivation, and awareness play a decisive role in managing cyber incidents. When employees operate within a supportive managerial environment and a culture of continuous learning, their adherence to secure behaviors and willingness to share cybersecurity knowledge naturally improve. Conversely, cultural weaknesses or poor communication between technical and managerial units may increase human errors and heighten system vulnerabilities. Moreover, the positive effects of the technical–instrumental and environmental–regulatory subsystems emphasize the importance of aligning technology with human behavior and maintaining dynamic regulatory frameworks. Although technology and security standards form the foundation of cyber defense, their long-term stability

and effectiveness depend on the synergy of organizational behaviors and learning-oriented processes. From a managerial perspective, the study's results suggest that the future direction of cybersecurity resilience in banking should move toward an integrated macro-ergonomic approach that aims to achieve systemic alignment among people, technology, structure, and the environment rather than focusing on minor technical fixes. Cybersecurity resilience in digital banking is a multidimensional concept rooted in the dynamic interplay of system-wide components.

Conclusion

This study demonstrates that enhancing cybersecurity resilience in digital banking systems requires a holistic socio-technical perspective. The proposed macro-ergonomic model confirmed that the organizational–structural subsystem plays a central role in maintaining system stability. Strengthening coordination, fostering a culture of collaboration, and improving managerial processes can mitigate financial risks from cyber threats more effectively than purely technological interventions alone.

Please cite this article as follows: Omidi N, Ghanbarzadeh H, Emami M, Omidi M. A Model Based on Macro-ergonomics to Improve Cybersecurity Resilience and Reduce Financial Risk in Digital Banking: A Mixed-Method Study. *Iran J Ergon*. 2026; 13(4): 307-317 DOI:10.53208/IJE.13.4.307

مجله ارگونومی
دوره ۱۳، شماره ۴، زمستان ۱۴۰۴، صفحات: ۳۱۷-۳۰۷
DOI: 10.53208/IJE.13.4.307
https://journal.iehfs.ir/
UMSHA Press

مقاله پژوهشی

ارائهٔ مدل ماکروارگونومی برای ارتقای تاب‌آوری امنیت سایبری با هدف کاهش ریسک مالی در بانکداری دیجیتال: مطالعهٔ آمیخته

نبی امیدی[۱]، حسن قنبرزاده[۲]، محسن امامی[۳]، محمدرضا امیدی[۴*]

[۱] گروه مدیریت، دانشگاه پیام نور، تهران، ایران
[۲] گروه مدیریت فناوری اطلاعات، دانشگاه آزاد اسلامی، واحد تهران جنوب، تهران، ایران
[۳] گروه مدیریت فناوری اطلاعات، دانشگاه آزاد اسلامی، واحد علوم تحقیقات، تهران، ایران
[۴] گروه مهندسی صنایع، دانشگاه پیام نور، تهران، ایران

تاریخ دریافت مقاله: ۱۴۰۴/۰۷/۰۸
تاریخ داوری مقاله: ۱۴۰۴/۱۰/۲۵
تاریخ پذیرش مقاله: ۱۴۰۴/۱۰/۲۶
تاریخ انتشار مقاله: ۱۴۰۴/۱۲/۲۹

* **نویسنده مسئول:** محمدرضا امیدی، گروه مهندسی صنایع، دانشگاه پیام نور، تهران، ایران

ایمیل: mromidi_91@yahoo.com

چکیده

اهداف: با گسترش فزایندهٔ بانکداری دیجیتال، تهدیدات سایبری به نوعی ریسک مالی و عملیاتی بزرگ تبدیل شده‌اند. این پژوهش با هدف طراحی مدلی مبتنی‌بر اصول ماکروارگونومی، برای تقویت تاب‌آوری امنیت سایبری به‌منظور کاهش ریسک مالی در صنعت بانکداری دیجیتال انجام شد.

روش کار: این پژوهش با رویکرد ترکیبی انجام شد. در فاز کیفی، با پانزده نفر خبره مصاحبه و داده‌ها با تحلیل تماتیک بررسی شد. در فاز کمی، مدل مفهومی حاصل از طریق پرسش‌نامه‌ای محقق‌ساخته روی نمونه‌ای شامل ۳۸۷ نفر از کارکنان بانک‌ها آزمون شد. تحلیل داده‌ها و ارزیابی مدل نهایی با استفاده از مدل‌سازی معادلات ساختاری (SEM) در نرم‌افزا LISREL صورت گرفت.

یافته‌ها: تحلیل کیفی به شناسایی ۵ مضمون اصلی و ۳۲ مضمون فرعی منجر شد که ابعاد مدل را تشکیل دادند: زیرسیستم فنی ـ ابزاری، انسانی ـ روان‌شناختی، سازمانی ـ ساختاری، عوامل محیطی ـ نظارتی و تاب‌آوری امنیت سایبری (پیامد). نتایج آزمون مدل کمی نشان داد که مدل برازش مطلوبی دارد (CMIN/DF=2.41؛ GFI = 0.92, CFI = 0.94, RMSEA = 0.061, SRMR = 0.057). هر چهار بُعد ماکروارگونومی تأثیر مثبت و معناداری در تاب‌آوری امنیت سایبری داشتند. در این میان، «زیرسیستم سازمانی-ساختاری» با ضریب مسیر استاندارد ۰/۴۸ بیشترین تأثیر را به خود اختصاص داد و به‌عنوان قوی‌ترین پیش‌بین شناسایی شد.

نتیجه‌گیری: مدل جامعه‌شناختی ـ فنی مبتنی‌بر ماکروارگونومی، چهارچوبی کارآمد برای تحلیل و تقویت تاب‌آوری امنیت سایبری در بانکداری دیجیتال ارائه می‌کند، به‌گونه‌ای که انتظار می‌رود افزایش تاب‌آوری سایبری، به کاهش ریسک‌های مالی نیز کمک کند. این نتیجه بر ضرورت گذار از رویکردهای صرفاً فنی به نگرشی سیستمی و تعاملی میان انسان، فناوری و ساختار سازمانی تأکید می‌کند.

کلید واژه‌ها: امنیت سایبری، بانکداری دیجیتال، تاب‌آوری، رویکرد جامعه‌شناختی-فنی، ماکروارگونومی

استناد: امیدی، نبی؛ قنبرزاده، حسن؛ امامی، محسن؛ امیدی، محمدرضا. ارائهٔ مدل ماکروارگونومی برای ارتقای تاب‌آوری امنیت سایبری با هدف کاهش ریسک مالی در بانکداری دیجیتال: مطالعهٔ آمیخته. مجله ارگونومی، زمستان ۱۴۰۴؛۱۳(۴): ۳۱۷-۳۰۷

مقدمه

در عصر دیجیتال، صنعت بانکداری با تحول پارادایمی مواجه است [۱]، درحالی‌که فناوری‌های نوین فرصت‌های بی‌سابقه‌ای برای نوآوری و ارائه خدمات ایجاد کرده‌اند، هم‌زمان سازمان‌ها را در معرض تهدیدات سایبری پیچیده و پویا قرار داده‌اند [۲]. رویکردهای سنتی به امنیت سایبری، که عمدتاً بر راه‌حل‌های فناورانه متمرکز بودند، دیگر برای مقابله با تهدیداتی که از تعاملات پیچیده میان انسان، فناوری و ساختارهای سازمانی نشئت می‌گیرند، کافی نیستند [۳]. این چالش نیاز به نگرش سیستمی و یکپارچه را برجسته می‌کند که

در آن، امنیت سایبری نه به‌عنوان مشکل فنی، بلکه به‌عنوان ویژگی بنیادی در سیستم جامعه‌شناختی ـ فنی درک می‌شود [۴].

علم ماکروارگونومی به‌عنوان نوعی رویکرد جامعه‌شناختی ـ فنی، به طراحی و بهینه‌سازی کل سیستم کار با هدف هماهنگ‌سازی زیرسیستم‌های انسانی، فنی و محیطی می‌پردازد [۵، ۶]. پژوهش‌ها نشان داده‌اند که مداخلات مبتنی‌بر ماکروارگونومی می‌تواند با بهبود متغیرهایی چون کار تیمی، ارتباطات و فرهنگ سازمانی، به ارتقای عملکرد کلی سیستم در بخش‌های مختلفی ازجمله زنجیرهٔ تأمین سلامت [۷] و صنایع گازی [۶] منجر شود. این اصول، فراتر از پیشگیری از اختلالات اسکلتی ـ عضلانی [۸] در کاهش استرس شغلی و بهبود سلامت روانی کارکنان نیز تأثیرگذار است [۹]؛ عواملی که مستقیماً در میزان خطای انسانی در فرایندهای امنیتی اثر می‌گذارند.

مفهوم کلیدی دیگر در این پژوهش، تاب‌آوری امنیت سایبری است [۱۰] که به معنای توانایی یک سیستم برای پیش‌بینی، مقاومت، بازیابی و انطباق در برابر حملات سایبری است [۱۱]. در این پژوهش، «تاب‌آوری امنیت سایبری» به‌صورت توانایی سیستم بانکی در پیش‌بینی، مقاومت، بازیابی و انطباق مؤثر در برابر رویدادهای سایبری تعریف عملیاتی می‌شود، به‌گونه‌ای که ارزیابی آن بر پایهٔ ادراک کارکنان از اثربخشی فرایندهای فنی، انسانی و سازمانی در مواجهه با تهدیدات امنیتی استوار است. این مفهوم فراتر از دفاع صرف است و بر پایداری عملکرد سازمان در شرایط بحرانی تأکید دارد [۱۲].

مطالعات پیشین ارتباط میان اصول ماکروارگونومی و مهندسی تاب‌آوری را در صنایع تولیدی نشان داده‌اند و تأیید کرده‌اند که یکپارچه‌سازی این دو رویکرد به طراحی بهینه و کارآمدتر سیستم منجر می‌شود [۱۳]. بااین‌حال، باید توجه کرد که بهبود تاب‌آوری لزوماً به معنای افزایش خودکار ایمنی نیست، به‌ویژه زمانی که فشارهای عملکردی و مالی سیستم را به‌سمت اتخاذ تصمیمات پرریسک سوق می‌دهد [۱۴]. این تنش در صنعت بانکداری، که ماهیتی کاملاً مالی دارد، اهمیتی دوچندان می‌یابد. «کاهش ریسک مالی» در چهارچوب این پژوهش به‌صورت کاهش احتمال وقوع زیان‌های مستقیم یا غیرمستقیم ناشی از اختلالات سایبری بر سرمایه، درآمد یا اعتبار مالی بانک تعریف می‌شود. این مفهوم به‌صورت کمی سنجیده نشده، بلکه از دید خبرگان به‌عنوان پیامد منطقی افزایش تاب‌آوری سایبری در نظر گرفته شده است.

باوجود اهمیت روزافزون امنیت سایبری در بخش مالی، مرور پیشینهٔ پژوهش نشان می‌دهد که مطالعات پیشین عمدتاً بر دو محور محدود بوده‌اند: نخست، بر رویکردهای فناورانه به امنیت سایبری (مانند رمزنگاری یا دفاع مبتنی‌بر هوش مصنوعی) بدون درنظرگرفتن تعاملات انسانی؛ دوم، بر عامل انسانی به‌شکل مستقل و خارج از معماری کل سیستم. این پراکندگی رویکردها باعث شده است تا پیوند میان ابعاد فنی، انسانی و سازمانی در بررسی تاب‌آوری امنیت سایبری مغفول بماند.

غفلت از این رویکرد سیستمی می‌تواند به پیامدهای زیان‌باری منجر شود. طراحی نامناسب فرایندهای امنیتی (ضعف در طراحی شغل)، فرهنگ سازمانی بی‌تفاوت به امنیت و آموزش‌های ناکارآمد همگی می‌توانند به پدیده‌هایی مانند خستگی امنیتی، افزایش خطای انسانی و کندی در واکنش به حوادث امنیتی منجر شوند. هریک از این شکست‌ها در سیستم جامعه‌شناختی ـ فنی، مستقیماً به افزایش ریسک مالی، ازدست‌رفتن اعتماد مشتریان و آسیب‌های جدی به اعتبار سازمان ترجمه می‌شود.

بنابراین، این پژوهش با هدف پرکردن شکاف موجود، به‌دنبال طراحی نوعی مدل جامعه‌شناختی ـ فنی مبتنی‌بر اصول ماکروارگونومی برای تقویت تاب‌آوری امنیت سایبری است که به‌طور غیرمستقیم به کاهش ریسک مالی کمک کند. پرسش اصلی این پژوهش آن است که چگونه می‌توان با بهره‌گیری از اصول ماکروارگونومی، مدلی جامعه‌شناختی ـ فنی برای ارتقای تاب‌آوری امنیت سایبری در بانکداری دیجیتال طراحی کرد، به‌گونه‌ای که تقویت این تاب‌آوری به‌طور غیرمستقیم به کاهش ریسک‌های مالی منجر شود. نوآوری پژوهش در ترکیب رویکرد ماکروارگونومیک با تحلیل‌های تاب‌آوری سایبری در حوزهٔ مالی است؛ حوزه‌ای که تاکنون به‌صورت منسجم مطالعه نشده است.

روش کار

پژوهش حاضر با به‌کارگیری روش تحقیق ترکیبی (Mixed-Methods) و براساس طرح اکتشافی متوالی (Exploratory Sequential Design) به انجام رسید. در این چهارچوب، مطالعه در دو فاز اصلی و پیوسته اجرا شد؛ فاز نخست با ماهیت کیفی به شناسایی و استخراج ابعاد و مؤلفه‌های بنیادین مدل از طریق مصاحبه‌های عمیق با نخبگان اختصاص یافت که خروجی آن تدوین نوعی مدل مفهومی اولیه بود. در ادامه، فاز دوم با ماهیت کمی، با هدف آزمون، اعتبارسنجی و برازش مدل مفهومی حاصل از فاز کیفی، از طریق ابزار پرسش‌نامه و تحلیل آن در یک جامعهٔ آماری گسترده‌تر به اجرا درآمد. این توالی روش‌شناختی این امکان را فراهم کرد تا ابتدا درکی عمیق و غنی از پدیدهٔ مورد مطالعه شکل گیرد و سپس یافته‌های کیفی به مدلی قابل تعمیم و آزمون‌پذیر تبدیل شود.

در فاز کیفی پژوهش، که با رویکرد پدیدارشناسی تفسیری انجام شد، هدف اصلی شناسایی عوامل کلیدی مدل بود. در این پژوهش «تاب‌آوری امنیت سایبری» به‌عنوان متغیر پیامد اصلی در نظر گرفته شد. با توجه به اینکه در فاز کیفی، خبرگان این مفهوم را قویاً با «کاهش ریسک مالی» پیوند دادند، این دو به‌عنوان هدف یکپارچه در نظر گرفته شدند؛ زیرا تاب‌آوری مؤثر ذاتاً به کاهش ریسک‌های مالی منجر می‌شود. جامعهٔ این بخش شامل نخبگان دانشگاهی و خبرگان صنعتی در چهار حوزهٔ ارگونومی، امنیت سایبری، مدیریت مالی و مدیریت فناوری در ایران بود. نمونه‌گیری به‌صورت هدفمند ـ قضاوتی آغاز شد و با تکنیک گلوله‌برفی تا رسیدن به اشباع نظری ادامه یافت که پس از پانزده مصاحبهٔ نیمه‌ساختاریافته محقق شد. معیارهای ورود عبارت بودند از: حداقل ده سال سابقهٔ مرتبط یا مدرک دکتری/ تصدی

سمت مدیریتی ارشد و تمایل آگاهانه به مشارکت. هر مصاحبه حدوداً شصت دقیقه ضبط و پیاده‌سازی شد، پرسش‌ها بر چالش‌های تعامل انسان ـ فناوری و نقش ساختار و فرهنگ سازمانی در تاب‌آوری و پیوند شکست‌های امنیتی با ریسک مالی متمرکز بود و داده‌ها با تحلیل مضمون براون و کلارک در MAXQDA 2020 تحلیل و ابعاد مدل مفهومی اولیه استخراج شد.

فاز کمی مطالعه با روش توصیفی ـ پیمایشی و با هدف آزمون مدل مفهومی تدوین‌شده اجرا شد. جامعهٔ آماری این بخش تمام کارکنان ستادی بانک‌های دولتی و خصوصی شهر تهران در سال ۱۴۰۴ بودند که وظایفشان با حوزه‌های فناوری اطلاعات، امنیت، مدیریت ریسک و عملیات دیجیتال ارتباط داشت. حجم نمونه با استفاده از فرمول کوکران و با درنظرگرفتن سطح اطمینان ۹۵ درصد، ۳۸۵ نفر محاسبه و به‌منظور پوشش موارد ریزش احتمالی، ۴۰۰ پرسش‌نامه توزیع شد. علاوه‌بر تعیین حجم نمونهٔ اولیه با فرمول کوکران، به‌منظور اطمینان از کفایت نمونه برای تحلیل مدل‌سازی معادلات ساختاری (SEM)، یک تحلیل توان آماری پسینی (Post-hoc) با استفاده از نرم‌افزار G*Power انجام شد.

با درنظرگرفتن حجم نمونهٔ نهایی (N=387)، تعداد متغیرهای مکنون پیش‌بین (۴ متغیر) و متغیرهای مشاهده‌شده در مدل (۳۲ گویه) و با فرض اندازهٔ اثر متوسط ($f^2 = ۰/۱۵$) در سطح معناداری α=۰/۰۵، نتایج نشان داد که توان آماری پژوهش تقریباً برابر با ۰/۹۹ است. این مقدار بسیار بالاتر از حداقل توان قابل قبول (۰/۸۰) است و نشان می‌دهد که حجم نمونهٔ پژوهش برای شناسایی روابط معنادار در مدل ساختاری، کفایت بسیار بالایی داشته است. روش نمونه‌گیری خوشه‌ای چندمرحله‌ای بود؛ به این ترتیب که ابتدا پنج بانک به‌صورت تصادفی انتخاب، سپس از هر بانک چهار واحد ستادی برگزیده و در نهایت، نمونه‌گیری در دسترس انجام شد.

ابزار اصلی گردآوری داده‌ها در فاز کمی، پرسش‌نامهٔ محقق‌ساخته بود که فرایند طراحی و اعتبارسنجی آن در چند مرحله انجام شد:

۱. تولید گویه‌ها: گویه‌های اولیهٔ پرسش‌نامه مستقیماً از مضامین فرعی و اصلی استخراج‌شده در فاز کیفی تولید شدند. به این صورت که برای هریک از مؤلفه‌های شناسایی‌شده در مدل مفهومی، چندین گویه طراحی شد تا آن مفهوم را به شکلی قابل سنجش در مقیاس پنج‌درجه‌ای لیکرت (از ۱=کاملاً مخالفم تا ۵=کاملاً موافقم) ارزیابی کنند. هدف این بود که هر گویه به‌روشنی به یکی از ابعاد نظری مدل متصل باشد.

۲. ارزیابی روایی محتوا و صوری: نسخهٔ اولیه پرسش‌نامه در اختیار یک پنل ده‌نفره از خبرگان دانشگاهی و صنعتی (شامل پنج نفر از شرکت‌کنندگان در فاز کیفی) قرار گرفت. از ایشان خواسته شد تا هر گویه را از منظر وضوح، مرتبط‌بودن با سازه و ابهام‌نداشتن ارزیابی کنند و اصلاحات پیشنهادی خود را ارائه دهند. پس از دو دور بازبینی و اعمال نظر، روایی محتوایی و صوری ابزار مورد تأیید پنل قرار گرفت.

۳. اجرای مطالعهٔ راهنما و سنجش پایایی: پس از نهایی‌سازی گویه‌ها، پرسش‌نامه روی نمونهٔ اولیهٔ سی‌نفره از کارکنان ستادی بانک (خارج از نمونهٔ اصلی) توزیع شد. سپس پایایی ابزار با استفاده از ضریب آلفای کرونباخ برای هریک از سازه‌های مدل به‌صورت جداگانه محاسبه شد. نتایج نشان داد که ضریب آلفا برای تمامی سازه‌ها بالاتر از مقدار قابل قبول ۰/۷ بود که حاکی از همسانی درونی مطلوب گویه‌هاست.

برای آزمون مدل مفهومی پژوهش از رویکرد مدل‌سازی معادلات ساختاری مبتنی‌بر کوواریانس (CB-SEM) با استفاده از نرم‌افزار LISREL نسخه ۸.۸ استفاده شد. برای ارزیابی برازش مدل کلی، از شاخص‌های مطلق، تطبیقی و مقتصد (Parsimonious) بهره گرفته شد. این شاخص‌ها عبارت‌اند از: کای-اسکوئر به درجهٔ آزادی (χ^2/df)، شاخص نیکویی برازش (GFI)، شاخص برازش تطبیقی (CFI)، ریشهٔ میانگین مربعات خطای تقریب (RMSEA) و ریشهٔ میانگین مربعات باقی‌ماندهٔ استانداردشده (SRMR). معیارهای پذیرش برای برازش مطلوب مدل شامل مقادیر کمتر از ۳ برای χ^2/df، مقادیر بزرگ‌تر از ۰/۹۰ برای GFI و CFI و مقادیر کوچک‌تر از ۰/۰۸ برای RMSEA و SRMR در نظر گرفته شد.

یافته‌ها

در فاز کیفی، پانزده نخبه و کارشناس ارشد شرکت کردند که ۸۰ درصد (دوازده نفر) مرد و ۲۰ درصد (سه نفر) زن بودند؛ ۸۶/۷ درصد (سیزده نفر) دارای مدرک دکتری و میانگین سابقهٔ کاری بیش از پانزده سال بودند و از لحاظ حوزهٔ تخصصی به‌صورت متوازن، از ارگونومی (چهار نفر)، امنیت سایبری (چهار نفر)، مدیریت مالی (چهار نفر) و مدیریت فناوری (سه نفر) انتخاب شده بودند. در فاز کمی، از ۴۰۰ پرسش‌نامهٔ توزیع‌شده، ۳۸۷ پرسش‌نامه کامل برگشت (نرخ بازگشت ۹۶/۷۵ درصد). نمونه شامل ۵۶/۸ درصد (۲۲۰ نفر) مرد و ۴۳/۲ درصد (۱۶۷ نفر) زن بود، بیشترین فراوانی سنی در گروه ۳۱ تا ۴۰ سال (۴۵/۲ درصد) و بیشترین سطح تحصیلات مربوط به کارشناسی (۵۱/۴ درصد) و کارشناسی ارشد (۳۸ درصد) بود. واحدهای مشارکت‌کننده عمدتاً فناوری اطلاعات و امنیت (۳۵/۴ درصد)، مدیریت ریسک و تطبیق (۲۲ درصد) و عملیات بانکداری دیجیتال (۱۹/۶ درصد) بودند که نشان‌دهندهٔ تنوع و قابلیت تعمیم مناسب در سطح ستادی بانک‌هاست. جزئیات کامل در جدول ۱ آمده است.

داده‌های پانزده مصاحبه با روش تحلیل مضمون شش‌مرحله‌ای براون و کلارک پردازش شد. پس از چندبار خوانش متن‌ها و ثبت برداشت‌ها، با کدگذاری خط‌به‌خط، ۲۱۴ کد اولیه استخراج شد که در مراحل بعدی ادغام و دسته‌بندی شد و به‌صورت ۳۲ مضمون فرعی سازمان‌دهی شد. در نهایت، این مضامین فرعی تحت ۵ مضمون اصلی قرار گرفتند: «زیرسیستم فنی ـ ابزاری»، «زیرسیستم انسانی ـ روان‌شناختی»، «زیرسیستم سازمانی ـ ساختاری»، «عوامل محیطی و نظارتی» و «تاب‌آوری امنیت سایبری و کاهش ریسک مالی». این چهارچوب مفهومی پایهٔ طراحی پرسش‌نامهٔ فاز کمی بود و جزئیات کامل مضامین در جدول ۲ ارائه شده است.

جدول ۱: ویژگی‌های جمعیت‌شناختی شرکت‌کنندگان در فاز کیفی و کمی

متغیر	گروه/سطح	فراوانی (n)	درصد (٪)
فاز کیفی (N=15)			
جنسیت	مرد	۱۲	۸۰/۰
	زن	۳	۲۰/۰
سطح تحصیلات	دکتری تخصصی	۱۳	۸۶/۷
	کارشناسی ارشد	۲	۱۳/۳
سابقهٔ کاری (سال)	۱۰ تا ۱۵ سال	۴	۲۶/۷
	بیش از ۱۵ سال	۱۱	۷۳/۳
حوزهٔ تخصصی	ارگونومی، امنیت سایبری، مدیریت مالی	هر کدام چهار نفر	۸۰/۰
	مدیریت فناوری	۳	۲۰/۰
فاز کمی (N=387)			
جنسیت	مرد	۲۲۰	۵۶/۸
	زن	۱۶۷	۴۳/۲
سن (سال)	کمتر از ۳۰ سال	۶۵	۱۶/۸
	۳۱ تا ۴۰ سال	۱۷۵	۴۵/۲
	۴۱ تا ۵۰ سال	۱۱۲	۲۹/۰
	بیش از ۵۰ سال	۳۵	۹/۰
سطح تحصیلات	کارشناسی	۱۹۹	۵۱/۴
	کارشناسی ارشد	۱۴۷	۳۸/۰
	دکتری	۴۱	۱۰/۶
سابقهٔ کاری (سال)	کمتر از ۵ سال	۷۸	۲۰/۰
	۵ تا ۱۰ سال	۱۴۰	۳۶/۲
	بیش از ۱۰ سال	۱۶۹	۴۳/۶

جدول ۲: مضامین اصلی و فرعی استخراج‌شده از تحلیل کیفی

مضمون اصلی (Organizing Theme)	مضامین فرعی (Sub-themes)
۱. زیرسیستم فنی ـ ابزاری (Technical Subsystem)	۱. طراحی کاربرمحور ابزارهای امنیتی (UX/UI)، ۲. یکپارچگی و سازگاری سیستم‌ها، ۳. اتوماسیون فرایندهای امنیتی، ۴. به‌کارگیری هوش مصنوعی در کشف تهدید، ۵. استحکام زیرساخت‌های فنی، ۶. مدیریت متمرکز هویت و دسترسی
۲. زیرسیستم انسانی ـ روان‌شناختی (Human Subsystem)	۷. آگاهی و دانش امنیت سایبری، ۸. مدیریت بار شناختی کارکنان، ۹. انگیزش و تعهد به سیاست‌های امنیتی، ۱۰. ادراک ریسک و حساسیت به تهدید، ۱۱. فرهنگ گزارش‌دهی خطا و حوادث، ۱۲. مهارت‌های تصمیم‌گیری تحت فشار، ۱۳. مقاومت در برابر خستگی امنیتی
۳. زیرسیستم سازمانی ـ ساختاری (Organizational Subsystem)	۱۴. حمایت مدیریت ارشد، ۱۵. طراحی ارگونومیک مشاغل و فرایندها، ۱۶. ارتباطات و همکاری بین‌واحدی، ۱۷. تخصیص بهینهٔ منابع (مالی و انسانی)، ۱۸. ساختار سازمانی منعطف و پاسخ‌گو، ۱۹. نظام ارزیابی عملکرد و پاداش مبتنی‌بر امنیت، ۲۰. شفافیت در سیاست‌ها و رویه‌های امنیتی، ۲۱. آموزش‌های مستمر و شبیه‌سازی حملات
۴. عوامل محیطی و نظارتی (Environmental Factors)	۲۲. الزامات و قوانین رگولاتوری، ۲۳. پویایی و پیچیدگی تهدیدات خارجی، ۲۴. همکاری و اشتراک اطلاعات با نهادهای بیرونی، ۲۵. فشار رقابتی بازار، ۲۶. مدیریت ریسک تأمین‌کنندگان و پیمانکاران
۵. تاب‌آوری امنیت سایبری و کاهش ریسک مالی (Outcome)	۲۷. قابلیت پیش‌بینی و پیشگیری از حملات، ۲۸. قابلیت مقاومت و تداوم خدمت حین حمله، ۲۹. قابلیت بازیابی سریع پس از حادثه، ۳۰. قابلیت یادگیری و انطباق با تهدیدات جدید، ۳۱. کاهش خسارات مالی مستقیم و غیرمستقیم، ۳۲. حفظ اعتماد مشتری و اعتبار برند

پیش از آزمون مدل ساختاری، مدل اندازه‌گیری با CFA سنجیده شد که شاخص‌های برازش کلی مطلوب بود ($\chi^2/df=2.18$, GFI=0.91, CFI=0.95, RMSEA=0.055, SRMR=0.051). بررسی روایی همگرا و پایایی نشان داد که بارهای عاملی همهٔ سازه‌ها بالاتر از ۰/۵ و در بازه‌های زیر قرار دارند: زیرسیستم فنی ـ ابزاری (بارها ۰/۷۱-۰/۸۵، α=0.88، CR=0.89، AVE=0.62)، زیرسیستم انسانی ـ روان‌شناختی (بارها ۰/۷۰-۰/۸۸، α=0.90، CR=0.91، AVE=0.65)، زیرسیستم سازمانی

ـ ساختاری (بارها ۰/۷۵-۰/۹۰، α=0.92، CR=0.93، AVE=0.70)، عوامل محیطی و نظارتی (بارها ۰/۶۸-۰/۸۱، α=0.85، CR=0.86، AVE=0.58) و تاب‌آوری و کاهش ریسک (بارها ۰/۷۸-۰/۸۶، α=0.91، CR=0.92، AVE=0.68). بنابراین، همهٔ سازه‌ها از نظر روایی همگرا و پایایی در سطح مطلوب قرار دارند.

پس از تأیید روایی و پایایی مدل اندازه‌گیری، گام بعدی آزمون مدل ساختاری پژوهش به‌منظور ارزیابی برازش کلی و بررسی فرضیه‌ها بود. برای این منظور، مجموعه‌ای از شاخص‌های برازش مطلق، تطبیقی و مقتصد محاسبه شد تا اطمینان حاصل شود که مدل مفهومی با داده‌های جمع‌آوری‌شده سازگاری دارد. همان‌طور که نتایج جدول ۳ نشان می‌دهد، تمامی شاخص‌های کلیدی در محدودهٔ قابل قبول قرار دارند. نسبت کای-اسکوئر به درجهٔ آزادی (۲/۴۱) نشان‌دهندهٔ عدم مغایرت شدید مدل با داده‌هاست. شاخص‌های GFI (۰/۹۲) و CFI (۰/۹۴) برازش بسیار خوب مدل را تأیید می‌کنند و مقادیر RMSEA (۰/۰۶۱) و SRMR (۰/۰۵۷) نیز در سطح مطلوبی قرار دارند. مجموع این شواهد برازش ساختاری قوی مدل مفهومی پژوهش را تأیید و اعتبار لازم برای آزمون فرضیه‌ها را فراهم می‌کنند.

جدول ۳: نتایج شاخص‌های برازش مدل ساختاری پژوهش

شاخص برازش	نماد	مقدار محاسبه‌شده	معیار پذیرش	نتیجه
کای-اسکوئر به درجهٔ آزادی	χ^2/df	۲/۴۱	کمتر از ۳	برازش مطلوب
شاخص نیکویی برازش	GFI	۰/۹۲	بزرگ‌تر از ۰/۹۰	برازش مطلوب
شاخص برازش تطبیقی	CFI	۰/۹۴	بزرگ‌تر از ۰/۹۰	برازش مطلوب
ریشهٔ میانگین مربعات خطای تقریبی	RMSEA	۰/۰۶۱	کمتر از ۰/۰۸	برازش مطلوب
ریشهٔ میانگین مربعات باقی‌مانده استانداردشده	SRMR	۰/۰۵۷	کمتر از ۰/۰۸	برازش مطلوب

پس از تأیید برازش کلی مدل، فرضیه‌ها از طریق بررسی ضرایب مسیر استاندارد (Beta)، آمارهٔ تی (T-Value) و سطح معناداری (P-Value) آزمون شدند. نتایج حاکی از آن بود که هر چهار بُعد پیش‌بین مدل شامل «زیرسیستم فنی ـ ابزاری»، «زیرسیستم انسانی-روان‌شناختی»، «زیرسیستم سازمانی ـ ساختاری» و «عوامل محیطی و نظارتی» تأثیر مثبت و معناداری بر متغیر وابسته، یعنی «تاب‌آوری امنیت سایبری و کاهش ریسک مالی» داشتند. در این میان، «زیرسیستم سازمانی ـ ساختاری» با ضریب مسیر ۰/۴۸، بیشترین تأثیر را به خود اختصاص داد که نشان‌دهندهٔ نقش کلیدی فرهنگ، حمایت مدیریت و طراحی بهینه فرایندها در دستیابی به اهداف مدل است. جزئیات کامل نتایج آزمون فرضیه‌ها در جدول ۴ ارائه شده است.

جدول ۴: نتایج مدل‌سازی برای آزمون فرضیه‌های پژوهش

مسیر فرضیه (از متغیر مستقل به وابسته)	ضریب مسیر استاندارد(Beta)	آمارهٔ تی (T-Value)	سطح معناداری (P-Value)	نتیجه
زیرسیستم انسانی ـ روان‌شناختی ← تاب‌آوری و کاهش ریسک	۰/۲۷	۴/۸۱	۰/۰۰۱	تأیید شد
زیرسیستم فنی ـ ابزاری ← تاب‌آوری و کاهش ریسک	۰/۳۵	۶/۱۴	۰/۰۰۰	تأیید شد
زیرسیستم سازمانی ـ ساختاری ← تاب‌آوری و کاهش ریسک	۰/۴۸	۷/۹۲	۰/۰۰۰	تأیید شد
عوامل محیطی و نظارتی ← تاب‌آوری و کاهش ریسک	۰/۲۱	۳/۵۶	۰/۰۱۲	تأیید شد

بحث

یافتهٔ اصلی این پژوهش موفقیت در طراحی و اعتبارسنجی نوعی مدل یکپارچه مبتنی‌بر رویکرد جامعه‌شناختی ـ فنی ماکروارگونومی برای تقویت تاب‌آوری امنیت سایبری و کاهش ریسک مالی بود. این یافته نشان می‌دهد که امنیت سایبری در بانکداری دیجیتال، پدیده‌ای صرفاً فناورانه نیست، بلکه یک خروجی سیستمی است که از تعامل پیچیده میان انسان، فناوری، ساختار سازمانی و محیط بیرونی نشئت می‌گیرد. موفقیت این مدل در تبیین متغیر وابسته، با پژوهش Azadeh و همکاران همسو است که نشان دادند ادغام اصول مهندسی تاب‌آوری و ماکروارگونومی به بهبود کارایی کلی سیستم در کارخانه‌های صنعتی منجر می‌شود [۱۳]. همان‌طور که در آن پژوهش، یکپارچه‌سازی این دو رویکرد به طراحی بهینه سیستم منتج شد، در پژوهش حاضر نیز رویکرد ماکروارگونومی توانست چهارچوبی مؤثر برای طراحی یک سیستم دفاعی مقاوم در برابر تهدیدات سایبری فراهم کند. این موضوع قابلیت تعمیم رویکرد ماکروارگونومی را از محیط‌های صنعتی و تولیدی به حوزه‌های خدماتی و فناورانه مانند بانکداری دیجیتال تأیید می‌کند.

مهم‌ترین یافتهٔ پژوهش حاضر آن بود که «زیرسیستم سازمانی ـ ساختاری» با بالاترین ضریب مسیر (۰/۴۸)، قوی‌ترین پیش‌بین برای تاب‌آوری امنیت سایبری شناخته شد. این نتیجه‌گیری بر این واقعیت تأکید می‌کند که عواملی مانند فرهنگ امنیت، حمایت مدیریت ارشد، شفافیت در رویه‌ها و ارتباطات سازمانی مؤثر، بیش از هر عامل دیگری در شکل‌دهی به اکوسیستم سایبری امن نقش دارند. این یافته به شکل قابل توجهی با نتایج Azadeh و همکاران که «کار تیمی» را مؤثرترین

عامل ماکروارگونومی در زنجیرهٔ تأمین سلامت شناسایی کردند [۱۵] و همچنین با پژوهش حسن‌زاده و همکاران که «دستورالعمل‌ها و آموزش» و «ارتباطات مناسب» را کلیدی‌ترین عوامل در بهبود ایمنی و بهره‌وری در یک پالایشگاه گاز دانستند [۶] هم‌سو است. در هر سه مطالعه، با وجود تفاوت در حوزهٔ کاربرد (بانکداری، سلامت، صنعت گاز)، متغیرهای مرتبط با ساختار، فرایندها و تعاملات سازمانی سنگ بنای بهبود عملکرد سیستم شناخته شده‌اند.

دومین یافتهٔ برجسته، تأثیرگذاری زیاد «زیرسیستم فنی ـ ابزاری» بر تاب‌آوری سایبری بود. این نتیجه نشان می‌دهد که طراحی ابزارها، سامانه‌ها و رابط‌های کاربری به شیوه‌ای که با قابلیت‌ها و محدودیت‌های شناختی انسان سازگار باشد، در کاهش خطاهای انسانی و تقویت خطوط دفاعی دیجیتال نقشی حیاتی ایفا می‌کند. این بُعد مستقیماً با دغدغه‌های اصلی ارگونومی در تطبیق کار با انسان مرتبط است. این یافته همسو با پژوهش Mansoor و همکاران قرار می‌گیرد که بر لزوم تنظیمات ارگونومیک در تجهیزات و محیط برای پیشگیری از آسیب‌های اسکلتی ـ عضلانی در میان متخصصان مراقبت‌های بهداشتی تأکید کردند [۸]. همچنین، مطالعهٔ Almada و Renner که مسائل مربوط به طراحی وسایل حمل‌ونقل عمومی را برای کاربران ویلچر تحلیل کرد، نشان داد که طراحی نامناسب محیط فیزیکی (فنی) مانع اصلی دسترسی‌پذیری است [۱۶]. پژوهش حاضر این منطق را به حوزهٔ دیجیتال بسط می‌دهد و استدلال می‌کند که طراحی ضعیف ابزارهای دیجیتال مانعی کلیدی در برابر عملکرد امن کارکنان است.

یافتهٔ دیگر پژوهش تأثیر مثبت و معنادار «زیرسیستم انسانی ـ روان‌شناختی» در متغیر وابسته بود. این نتیجه مؤید آن است که ویژگی‌های فردی کارکنان مانند سطح آگاهی، انگیزه، استرس شغلی و نگرش آن‌ها به امنیت، به‌طور مستقیم در رفتار ایمن آن‌ها و در نتیجه بر کل تاب‌آوری سیستم تأثیر می‌گذارد. این یافته با نتایج مطالعهٔ Super و همکاران، که ارتباط مستقیم میان عوامل سلامت روان (مانند استرس و اضطراب) و عملکرد تیم‌های حرفه‌ای را در بخش مراقبت‌های ویژه (ICU) نشان دادند، کاملاً هم‌خوانی دارد [۳]. همان‌طور که در آن مطالعه، عوامل روان‌شناختی در همکاری و عملکرد تیمی در محیط پرخطر تأثیرگذار بود، در این پژوهش نیز مشخص شد که وضعیت روانی و شناختی کارکنان عامل تعیین‌کننده‌ای در عملکرد آن‌ها در محیط پرریسک دیجیتال است. علاوه‌بر این، همسو با دیدگاه Zayas-Cabán و Rogers که بر لزوم درک «ارگونومی بیمار» برای بهبود مشارکت در تحقیقات سلامت تأکید دارند [۱۷]، یافتهٔ ما نیز بر ضرورت درک «ارگونومی کارمند» برای بهبود مشارکت او در فرایندهای امنیتی تأکید می‌کند.

نتایج نشان داد که «عوامل محیطی و نظارتی» نیز بر تاب‌آوری امنیت سایبری تأثیر معناداری دارند، هرچند شدت این تأثیر کمتر از سه بُعد دیگر بود. این یافته را می‌توان این‌گونه تفسیر کرد که الزامات قانونی، استانداردها و فشارهای نهادی از سوی رگولاتورها، چهارچوب و حداقل‌های لازم را برای اقدامات امنیتی تعیین می‌کنند، اما دستیابی به سطح مطلوبی از تاب‌آوری، بیش از آنکه محصول فشارهای بیرونی باشد، نتیجهٔ بهینه‌سازی فرایندهای درونی سازمان (ساختار، فناوری و انسان) است. این نتیجه‌گیری با یافته‌های ضمنی حسن‌زاده و همکاران قابل مقایسه است که نشان دادند وضعیت ماکروارگونومی در بیمارستان‌های مختلف به‌طور معناداری متفاوت بود [۶] که این موضوع حاکی از آن است که باوجود یک محیط نظارتی یکسان (نظام سلامت)، تفاوت‌های داخلی سازمان‌ها نقش تعیین‌کننده‌تری در وضعیت ارگونومیک و سلامت کارکنان ایفا می‌کند.

در نهایت، قدرت حقیقی مدل ارائه‌شده نه در تأثیر مجزای هریک از ابعاد، بلکه در ماهیت یکپارچه و تعاملی آن‌ها نهفته است. تاب‌آوری امنیت سایبری یک ویژگی «برآینده» (Emergent Property) از یک سیستم جامعه‌شناختی ـ فنی هماهنگ است. این دیدگاه سیستمی با پژوهش Morel و همکاران، که رابطهٔ پیچیده میان ارگونومی، تاب‌آوری و ایمنی را در صنعت ماهیگیری بررسی کردند [۱۴]، ارتباط مفهومی عمیقی دارد. آن مطالعه به‌طور هشداردهنده‌ای نشان داد که بهبودهای ارگونومیک لزوماً به افزایش ایمنی منجر نمی‌شوند، بلکه ممکن است کارکنان برای افزایش عملکرد (صید بیشتر)، از آن‌ها استفاده کنند و درنتیجه، سطح ریسک ثابت بماند. این یافته یک نکتهٔ سیاستی مهم برای پژوهش حاضر به‌همراه دارد: اجرای موفقیت‌آمیز مدل ماکروارگونومی در بانکداری دیجیتال نیازمند آن است که هدف اصلی، یعنی «تاب‌آوری سایبری»، به‌وضوح در اولویت قرار گیرد تا بهبودهای حاصل از آن، صرفاً در خدمت اهداف عملکردی و مالی کوتاه‌مدت قرار نگیرد و به امنیت واقعی منجر شود.

این تحقیق نقشهٔ راه عملی برای گذار از رویکرد صرفاً فناورمحور به استراتژی جامعه‌شناختی ـ فنی مدیریتی ارائه می‌دهد. پیشنهاد می‌شود بانک‌ها ممیزی‌های «جامعه‌شناختی ـ فنی» را اجرا کنند که ابعاد انسانی، سازمانی و فنی را همراه با چک‌لیست‌های سنجش‌پذیر (مثلاً درصد کاهش کلیک روی ایمیل‌های فیشینگ یا تخصیص درصدی از بودجه IT به آموزش‌های تعاملی) اندازه‌گیری کند. تشکیل «کمیتهٔ راهبری تاب‌آوری سایبری» با نمایندگان فناوری، ریسک، منابع انسانی و عملیات و بازطراحی آموزش‌ها به‌صورت کارگاه‌های شبیه‌سازی حملهٔ مبتنی‌بر سناریو (با سنجه‌هایی مانند میانگین زمان شناسایی و بازیابی) از دیگر توصیه‌هاست. محدودیت‌ها شامل طبیعت مقطعی (که استنتاج علی را محدود می‌کند و مطالعات طولی را لازم می‌سازد)، نمونه‌گیری محدود به تهران (که به مطالعات تطبیقی در اقلیم‌ها و نوع بانک نیاز دارد) و اتکا به داده‌های خودگزارشی (که باید با شاخص‌های عینی مثل حوادث ثبت‌شده یا نتایج تست نفوذ ترکیب شود) است. همچنین بررسی نقش تعدیلگرهایی مانند اندازهٔ سازمان و سطح بلوغ دیجیتال برای تحقیقات آینده توصیه می‌شود.

نتیجه‌گیری

این پژوهش نشان می‌دهد که رویکرد ماکروارگونومی چهارچوبی کارآمد برای تقویت تاب‌آوری امنیت سایبری در بانکداری دیجیتال است. تاب‌آوری نتیجهٔ سیستم جامعه‌شناختی ـ فنی یکپارچه است

که زیرسیستم سازمانی ـ ساختاری به‌عنوان هسته و پیشران اصلی عمل می‌کند و تنها در هماهنگی با ابعاد فنی، انسانی و محیطی موفق است. بنابراین، انتقال از نگرش صرفاً فناورمحور به رویکرد سیستمی و انسان‌محور ضروری است و مدل پیشنهادی نقشهٔ راهی عملی برای مدیران به‌منظور طراحی محیط‌های کاری دیجیتال امن‌تر و کاهش ریسک مالی فراهم می‌آورد.

تشکر و قدردانی

بدین وسیله از تمامی نخبگان دانشگاهی و متخصصان صنعت بانکداری و همهٔ کارکنان محترم ستادی بانک‌ها که با صرف وقت و دقت، در تکمیل پرسش‌نامه‌ها ما را یاری کردند، صمیمانه سپاسگزاری می‌شود.

تضاد منافع

نویسندگان مقاله اعلام می‌کنند که هیچ‌گونه تضاد منافعی در انجام و انتشار نتایج این پژوهش وجود نداشته است.

مشارکت‌های نویسندگان

مفهوم‌سازی: نبی امیدی، محمدرضا امیدی

روش‌شناسی: نبی امیدی، حسن قنبرزاده

تحلیل: حسن قنبرزاده، محسن امامی

تحقیق: محسن امامی

مدیریت داده‌ها: محسن امامی

منابع: محسن امامی

نرم‌افزار: حسن قنبرزاده

تجسم: حسن قنبرزاده

اعتبارسنجی: محمدرضا امیدی

نظارت: محمدرضا امیدی

مدیریت پروژه: نبی امیدی

جذب سرمایه: غیرکاربردی

نوشتن –پیش‌نویس اصلی: نبی امیدی، محسن امامی

نگارش – بررسی و ویرایش: محمدرضا امیدی، حسن قنبرزاده

ملاحظات اخلاقی

این پژوهش با رعایت کامل اصول اخلاقی مبتنی‌بر بیانیهٔ هلسینکی و با اخذ کد اخلاق از کمیتهٔ پژوهش مربوطه انجام شد. پیش از شروع مصاحبه‌ها و توزیع پرسش‌نامه‌ها، رضایت‌نامهٔ آگاهانهٔ کتبی از تمامی شرکت‌کنندگان اخذ شد. در این رضایت‌نامه اهداف پژوهش، ماهیت داوطلبانهٔ مشارکت و حق خروج از مطالعه در هر زمان به‌طور کامل تشریح شد. به تمامی شرکت‌کنندگان اطمینان داده شد که اطلاعات آن‌ها به‌صورت کاملاً محرمانه باقی می‌ماند و نتایج صرفاً به شکل کلی و گروهی و بدون ذکر نام فرد یا سازمان تحلیل و منتشر خواهد شد.

حمایت مالی

این پژوهش با هزینهٔ شخصی محققان انجام شده و هیچ‌گونه حمایت مالی از هیچ سازمان یا نهاد دولتی یا خصوصی‌ای دریافت نکرده است.

REFERENCES

1. Tian S, Zhao B, Olivares RO. Cybersecurity risks and central banks' sentiment on central bank digital currency: Evidence from global cyberattacks. Fin Res Lett. 2023;53(C):103609. [DOI: 10.1016/j.frl.2022.103609]
2. Türegün N. Digital transformation and cybersecurity risks. Int J Account Inf Syst. 2025;56:100749. [DOI: 10.1016/j.accinf.2025.100749]
3. Super I, Zhang L, Wang B, Asan O. The impact of psychological factors on interprofessional team collaboration in the ICU: A macro-ergonomic case study. Appl Ergon. 2025;128:104535. [DOI: 10.1016/j.apergo.2025.104535] [PMID]
4. Qabajeh I, Thabtah F, Chiclana F. A recent review of conventional vs. automated cybersecurity anti-phishing techniques. Comput Sci Rev. 2018;29:44-55. [DOI: 10.1016/j.cosrev.2018.05.003]
5. Khoshakhlagh AH, Majdabadi MA, Yazdanirad S. The impact of ergonomic-educational interventions on reduction of musculoskeletal symptoms among employees of oil and gas installations in Iran. Work. 2022;71(3):651-60. [DOI: 10.3233/WOR-205231] [PMID]
6. Hassanzadeh P, Ghahramani A, Mohebbi I. An assessment of association between macro-ergonomics status and employees' prevalence of musculoskeletal disorders and job stress outcomes in Urmia educational and medical hospitals. Iran J Ergon. 2020;7(4):40-51. [DOI: 10.30699/jergon.7.4.40]
7. Rodríguez-Gámez IF, Maldonado-Macías AA, Lagarda-Leyva EA, Hernández-Arellano JL, Rodríguez Y. A Continuous Improvement Instrument for the evaluation of the ergonomics management system in the supply chain. Heliyon. 2024; 5;10(24):e40956. [DOI: 10.1016/j.heliyon.2024.e40956] [PMID]
8. Mansoor SN, Al Arabia DH, Rathore FA. Ergonomics and musculoskeletal disorders among health care professionals: Prevention is better than cure. J Pak Med Assoc. 2022;72(6):1243-5. [DOI: 10.47391/JPMA.22-76] [PMID]
9. Fu Y, Lu W, Chen J. A virtual reality-based ergonomic assessment approach for human-robot collaboration workstation design in modular construction manufacturing. Adv Eng Inform. 2025;64:103054. [DOI: 10.1016/j.aei.2024.103054]
10. Sulong Z, Fuszder MHR, Abdullah M, Abakah EJA. Cybersecurity risk and bank risk-taking. J Behav Exp Finance. 2025;47(C):101080. [DOI: 10.1016/j.jbef.2025.101080]
11. Chanda RC, Vafaei-Zadeh A, Hanifah H, Nikbin D. Assessing cybersecurity awareness among bank employees: A multi-stage analytical approach using PLS-SEM, ANN, and fsQCA in a developing country context. Comput Secur. 2025;149(C):104208. [DOI: 10.1016/j.cose.2024.10420]
12. Asmar M, Tuqan A. Integrating machine learning for sustaining cybersecurity in digital banks. Heliyon. 2024;10(17):e37571. [DOI: 10.1016/j.heliyon.2024.e37571] [PMID]
13. Azadeh A, Roudi E, Salehi V. Optimum design approach based on integrated macro-ergonomics and resilience engineering in a tile and ceramic factory. Saf Sci. 2017;96:62-74. [DOI: 10.1016/j.ssci.2017.02.017]
14. Morel G, Amalberti R, Chauvin C. How good micro/macro

ergonomics may improve resilience, but not necessarily safety. Saf Sci. 2009;47(2):285-94. [DOI: 10.1016/j.ssci.2008.03.002]
15. Azadeh A, Motevali Haghighi S, Gaeini Z, Shabanpour N. Optimization of healthcare supply chain in context of macro-ergonomics factors by a unique mathematical programming approach. Appl Ergon. 2016;55:46-55. [DOI: 10.1016/j.apergo.2016.01.002] [PMID]
16. Almada JF, Renner JS. Public transport accessibility for wheelchair users: a perspective from macro-ergonomic design. Work. 2015;50(4):531-41. [DOI: 10.3233/WOR-131811] [PMID]
17. Zayas-Cabán T, Rogers CC. The role of patient ergonomics in improving health research participation. Appl Ergon. 2025;125:104458. [DOI: 10.1016/j.apergo.2024.104458] [PMID].