Annals of Process Engineering and Management

www.apem.reapress.com

Ann. Proc. Eng. Manag. Vol. 2, No. 2 (2025) 69–75.

Paper Type: Original Article

Innovations and Cybersecurity Developments in Iranian Banks: A SWOT Analysis and Opportunity Comparison

Samira Azad Sanjari[1,*], Seyed Kamal Charsoughi[1]

[1] Department of Industrial and Systems Engineering, Tarbiat Modares University, Tehran, Iran; s.azadsanjari@modares.ac.ir; skch@modares.ac.ir.

Citation:

Received: 05 August 2024 *Revised: 13 December 2024* *Accepted: 25 February 2025*	Azad Sanjari, S., & Charsoughi, S, K. (2025). Innovations and cybersecurity developments in Iranian banks: A SWOT analysis and opportunity comparison. *Annals of process engineering and management, 2*(2), 69-75.

Abstract

Given the rapid growth of information and the significant increase in cyberattacks in recent years, evaluating and analyzing the state of information security in Iranian banks has become a critical necessity. According to security reports, banking malware and financial fraud have witnessed substantial growth over the past decades. In light of the increasing complexity of cyber threats and the high velocity of emerging risks, traditional security strategies are no longer sufficient to meet the evolving needs of Iranian banks. In this study, we employ the Strengths, Weaknesses, Opportunities, Threats (SWOT) framework to assess and analyze the cybersecurity landscape in Iran's banking sector. The use of SWOT enables us to formulate well-reasoned and evidence-based recommendations. Accordingly, this research utilizes SWOT analysis to identify effective solutions and robust strategic directions for strengthening cybersecurity in Iranian banking. Initially, we identify the internal strengths and weaknesses, as well as the external opportunities and threats that impact information security in Iranian banks. Based on the findings from the SWOT analysis, a set of strategic recommendations are proposed to enhance the cybersecurity posture of the country's banking system.

Keywords: Information security, SWOT, Risk assessment, Threats and vulnerabilities, Electronic banking.

1 | Introduction

An efficient banking system is indispensable for active participation in competitive markets and for engaging in electronic commerce activities. Beyond enhancing operational efficiency and productivity, digital technologies have fundamentally transformed the way financial services are conducted, how institutions communicate, and how they interact with the broader environment [1]. With the expansion of electronic services in financial and credit institutions, new types of risks and emerging threats have surfaced for banks [2].

Corresponding Author: s.azadsanjari@modares.ac.ir

https://doi.org/10.48314/apem.v2i2.29

The rapid growth of electronic banking services acts as a double-edged sword, creating both opportunities and vulnerabilities for financial institutions. Failure to properly identify and mitigate emerging risks in digital banking can negatively affect a bank's reputation and revenue streams, and may even pose threats to national security. According to recent cybersecurity reports, one such incident involved the potential leakage of customer data from 20 Iranian banks. The company TOSAN reportedly negotiated and made payments to IRLeaks to prevent the public release of the compromised data.

Over the past few decades, as infrastructures and technologies have evolved, the nature of international attacks has increasingly become cyber-based. Given Iran's strategic geopolitical standing, the country has become a focal point for such cyber offensives. According to a recent Kaspersky report in *Fig. 1*, Iran ranks fourth globally in ransomware infection rates based on data collected over the past month [3].

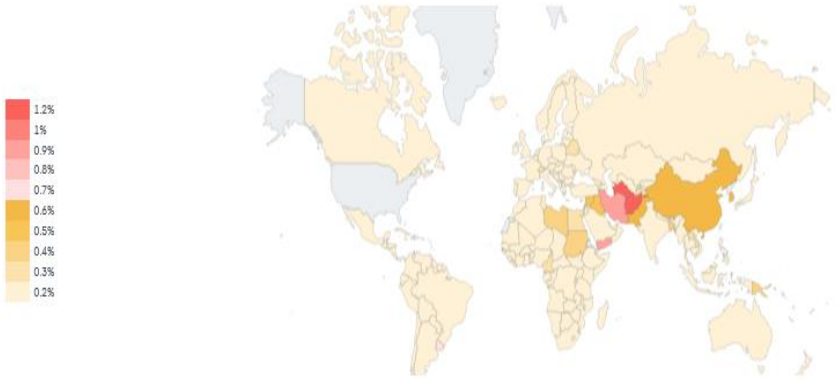

Fig. 2. Kaspersky report on the global ransomware infection landscape (Past month) [3].

According to the Global Cybersecurity Index (GCI) published by the International Telecommunication Union (ITU) [4], countries are evaluated based on their cybersecurity capabilities across five core dimensions. As illustrated in *Fig. 2*, Iran is currently positioned at Level 3 out of 5, indicating a developing stage in the implementation of cybersecurity measures [4]. However, to ascend to the ranks of global cybersecurity leaders and advance by two additional maturity levels, Iran must enhance its cybersecurity processes and frameworks.

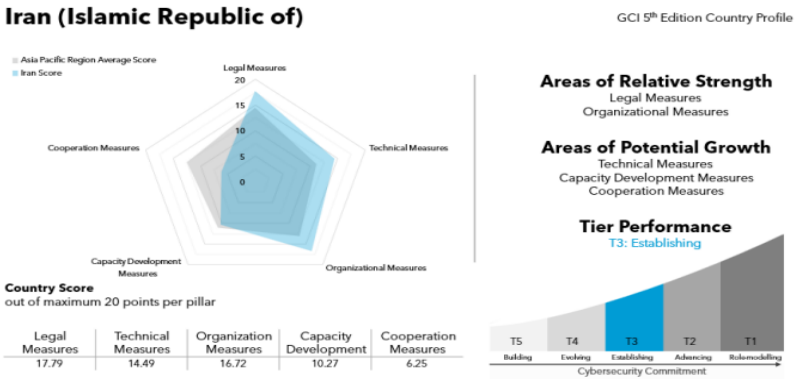

Fig. 2. Iran's cybersecurity compliance status based on the international telecommunication union global cybersecurity index 2024 report [4].

In addition, the fifth annual Sophos report [5]—which focuses on ransomware threats targeting financial institutions globally—reveals a sharp increase in such attacks over the past five years. In 2024, the volume of ransomware incidents reached its peak, with a 65% increase compared to previous years. As presented in *Fig. 3,* the ransom amounts demanded from financial institutions have imposed significant financial burdens.

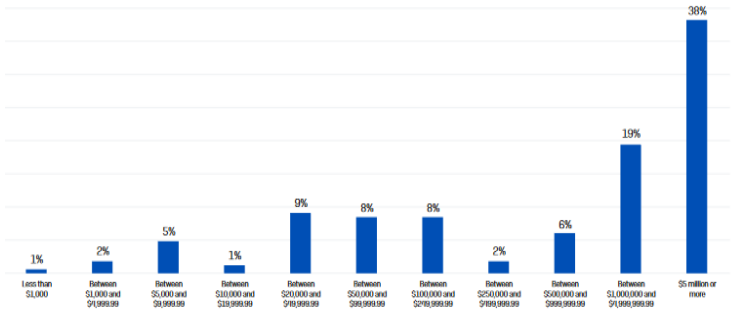

Fig. 3. Ransom demands from financial institutions by ransomware groups in 2024 [5].

Therefore, given the expanding landscape of cybersecurity threats in the banking sector, the assessment and analysis of information security risks in banks is of utmost importance. Identifying and prioritizing these risks can significantly mitigate their negative impacts on organizational operations. Moreover, recognizing potential opportunities and engaging in precise and well-structured strategic planning enables institutions to achieve their organizational goals effectively. In this proposed study, we investigate the current state of information security in Iranian banks.

To describe the research framework, the research methodology section provides the foundational concepts required for the study, including definitions of electronic banking, risk types, and Strengths, Weaknesses, Opportunities, Threats (SWOT) analysis. The research methodology section is followed by a literature review that discusses the current research landscape and highlights the ongoing challenges in information security. The Findings section presents the results of the SWOT analysis by identifying the strengths, internal weaknesses, external opportunities, and threats related to cybersecurity in Iranian banks. Finally, the conclusion outlines strategic recommendations and proposed solutions to enhance the current cybersecurity infrastructure.

2 | Research Methodology

Electronic banking refers to the provision of financial services through secure digital channels without requiring customers to be physically present at bank branches. This approach enables customers to perform financial transactions efficiently, saving time and cost [6]. Electronic banking encompasses services such as internet banking, mobile banking, telephone banking, ATM-based banking, electronic fund transfers, and card-based banking systems.

However, this mode of service delivery introduces several risks, including security risk, privacy risk, operational risk, reputational risk, legal risk, and strategic risk. Due to the adverse effects these risks may have on banks' capital and revenue, it is essential to forecast, assess, and mitigate them appropriately [7].

The SWOT analysis—an acronym for strengths, weaknesses, opportunities, and threats—is a strategic planning tool that organizations use to identify practical solutions and powerful strategies in their business operations. Because it provides an evaluative framework to assess both internal capabilities and external conditions, SWOT is widely applied across sectors.

For instance, Sousa et al. [8] employed SWOT analysis in the context of technology management in the agricultural industry, evaluating internal and external factors to support strategic planning. Similarly, researchers from the Department of Sociology at Usak University explored the application of SWOT as a robust strategy for security management, emphasizing its role in analyzing and formulating security frameworks [9].

In our research, we adopt the SWOT framework as a strategic planning approach to develop precise and well-grounded recommendations based on a comprehensive analysis. The strategic planning approach enables the

extraction of actionable insights regarding the future outlook of cybersecurity in Iran's electronic banking sector.

3 | Findings

One of the current significant challenges faced by banks is the development of strategic information security programs that align with the latest technological advancements. The SWOT analysis serves as a vital tool that helps banks understand their operational environment by identifying their internal strengths and weaknesses, as well as external opportunities and threats [10]. In this study, the cybersecurity status of Iranian banks has been examined, and the identified strengths, weaknesses, opportunities, and threats are outlined below.

3.1 | Strengths

Close collaboration with regulatory and supervisory bodies: Iranian banks benefit from their engagement with authoritative institutions such as the National Center for Cyberspace Security (AFTA), the Passive Defense Organization, and the Central Bank of Iran. These entities have established stringent regulations and standards for protecting customer information, which contributes to enhancing cybersecurity measures.

Strict internal policies and standards: Many banks in Iran implement standardized frameworks like ISO/IEC 27001 for information security management, which ensure structured approaches to risk handling and data protection [11].

Increased self-reliance and resilience under international sanctions: Sanctions have compelled banks to develop internal capacities and adopt indigenous solutions. This necessity has led to enhanced resilience and organizational sustainability in crisis scenarios.

Deployment of domestic platforms and technologies: Local knowledge-based companies have developed native systems for transaction processing, financial services, and security solutions. These localized systems reduce dependency on foreign technologies and minimize exposure to external threats.

3.2 | Weaknesses

Lack of alignment between organizational structure and international security standards: Several banks lack essential security governance units such as Information Security Committees, Red/Blue/Purple security teams, risk management departments, Security Operations Centers (SOC), and Incident Response Teams.

Insufficient infrastructure to counter advanced cyber threats: Many institutions still lack robust infrastructures required to defend against Advanced Persistent Threats (APTs). There is also a lack of proper implementation of security systems aligned with internationally recognized standards and best practices, such as those from SANS Institute and the Center for Internet Security (CIS) [12].

Limited access to cutting-edge technologies: Due to ongoing international sanctions, access to advanced security software and tools is restricted. This limitation has, in some cases, led to outdated systems that are unable to cope with rapidly evolving threats.

Shortage of specialized human capital: The emigration of skilled professionals in recent years has exacerbated the talent gap in the cybersecurity and IT sectors. This talent drain risks reducing operational efficiency and weakening the capacity to implement and sustain security protocols.

Inadequate employee training and awareness: Many employees lack awareness of cybersecurity threats and proper countermeasures. This gap often results in human error being exploited by attackers. A notable example is the Stuxnet malware incident, which exploited human error to infiltrate isolated nuclear infrastructure in Iran [13].

3.3 | Opportunities

Rapid growth in Artificial Intelligence (AI)-based security technologies: The increasing availability of artificial intelligence-powered tools presents a significant opportunity for enhancing threat detection and response. These technologies can analyze large-scale datasets to detect anomalies and recognize emerging and sophisticated cyber threats quickly. Additionally, the use of blockchain technology is gaining attention for its potential to secure data and transactions [10].

Rising public awareness of information security: As cybersecurity gains prominence in public discourse and media, general awareness around protecting personal and financial data is improving. The rise in high-profile cyberattacks and their economic and reputational consequences has also led to a greater emphasis on IT security within the banking sector.

Partnerships with domestic cybersecurity firms and adoption of local platforms: A growing number of Iranian tech companies specialize in information security. Collaborating with these firms through outsourcing, consultation, and deployment of indigenous technologies can improve the overall cybersecurity posture of banks.

Increased demand for electronic banking services: The expansion of digital and electronic banking in Iran creates opportunities for strengthening security in digital environments. Banks can capitalize on this trend to attract new customers and offer more secure services, provided that their digital infrastructure is reinforced [6].

New data protection regulations: The introduction of new national data protection laws offers a chance to upgrade security protocols and align with global best practices [14].

Leveraging the expertise of expatriate professionals: While brain drain is a challenge, maintaining relationships with Iranian professionals working in international tech firms can offer unique access to global cybersecurity expertise and best practices.

3.4 | Threats

Cyberattacks from foreign states and hacker groups: Iranian institutions face persistent threats from sophisticated external actors, including state-sponsored groups. These attacks may include Distributed Denial-of-Service (DDoS) attacks, phishing campaigns, or advanced malware. The objective may range from data theft to system disruption.

Inadequate data protection regulations: Although Iran has national laws in place, they lack the comprehensiveness and modernity of international frameworks such as the General Data Protection Regulation (GDPR). This regulatory gap may hinder effective defense against emerging threats [15].

Lag in adapting to technological change: Due to limitations in accessing cutting-edge technologies and persistent sanctions, Iranian banks often struggle to keep pace with rapid innovations in IT security.

Sanctions and international restrictions: Sanctions continue to limit Iran's access to advanced cybersecurity tools and platforms, weakening its defensive capabilities and widening the gap in security readiness compared to global standards.

Based on the comprehensive SWOT analysis, the summarized results of the cybersecurity status in Iranian banks are presented in *Table 1*.

Table 1. SWOT analysis summary of information security in Iranian banks.

	Internal	External
Positive	Strengths -Strong ties with regulatory and security authorities (e.g., Central Bank, AFTA) - Strict internal security standards and policies -Enhanced self-sufficiency and resilience under sanctions	Opportunities -Growing public awareness of information security -Collaboration with domestic cybersecurity companies and use of indigenous platforms -Increased demand for electronic banking services -Emergence of new data protection regulations -Leveraging the expertise of expatriate professionals -Rapid development of AI-based security technologies
Negative	Weaknesses -Organizational structures misaligned with security standards and missing key roles -Insufficient infrastructure to counter advanced threats (e.g., APTs) -Limited access to advanced knowledge and technologies -Slow processes for system updates -Shortage of specialized human resources -Over-reliance on local systems without regular modernization -Lack of cybersecurity awareness and training among staff -Limited budget and insufficient investment in cybersecurity	Threats -Cyberattacks by foreign states and hacking groups -Outdated or insufficient data protection regulations -Increase in internal attacks due to a lack of awareness or intentional misconduct -Low adaptability to rapid technological changes -International sanctions and restrictions -Patronage-based appointments

4 | Discussion and Conclusion

With the rapid growth of internet-based businesses and the expansion of electronic payment systems, cyber threats and online crimes have significantly increased. Given the critical role that banking systems play in maintaining national economic stability, the absence of a proactive and well-designed strategy for managing cyber crises could lead to serious systemic consequences. In light of the emergence of artificial intelligence and the increasing sophistication of cyberattacks, the development of a strategic information security program for banks is not only necessary but urgent for identifying and countering emerging threats.

A study conducted by a financial department in Ukraine analyzed the development of information technology in financial institutions using SWOT analysis to explore associated opportunities and threats [16]. Similarly, researchers from Usak University examined weaknesses, opportunities, and threats related to security management in a financial organization, providing insight into the structural challenges of cybersecurity [9]. More recently, in response to the growing influence of artificial intelligence, scholars have applied SWOT analysis to evaluate its implications for organizational management, identifying both opportunities and risks posed by AI-driven transformations [10].

In the present study, a comprehensive SWOT analysis was employed to identify the strengths, weaknesses, threats, and opportunities concerning information security in Iranian banks. Based on the findings, we propose a set of strategic recommendations aimed at enhancing the cybersecurity framework. These include upgrading national security standards and aligning with international frameworks, reinforcing digital infrastructure, adopting emerging AI-driven technologies, improving risk and vulnerability management, strengthening access control and data protection systems, instituting continuous monitoring and evaluation, conducting supplier and third-party security assessments, increasing security-related budgets and investments, and expanding training and awareness programs at both institutional and public levels.

Moreover, in today's rapidly evolving digital environment, the nature of cybersecurity challenges is becoming increasingly dynamic. Banks will likely encounter new forms of threats and opportunities that fall beyond the analytical scope of traditional SWOT models. Therefore, in addition to SWOT, a more holistic and adaptive strategic planning approach should be adopted to ensure a comprehensive cybersecurity roadmap.

Funding

The authors conducted this research independently without external financial support. All costs associated with this study were covered by the researchers' institutional resources.

Declaration of Interests

The authors affirm that there are no competing interests—financial, professional, or personal—that could influence the objectivity or outcomes of this research. This study was conducted with full academic ntegrity, free from any affiliations or relationships that might pose a conflict.

References

[1] Urbinati, A., Chiaroni, D., Chiesa, V., & Frattini, F. (2020). The role of digital technologies in open innovation processes: An exploratory multiple case study analysis. *R&d management*, *50*(1), 136–160. https://doi.org/10.1111/radm.12313

[2] Kshetri, N., Rahman, M. M., Sayeed, S. A., & Sultana, I. (2024). CryptoRAN: A review on cryptojacking and ransomware attacks wrt banking industry-threats, challenges, & problems. *2024 2nd international conference on advancement in computation & computer technologies (INCACCT)* (pp. 523–528). IEEE. https://doi.org/10.1109/InCACCT61598.2024.10550970

[3] Kaspersky. (2024). *Cybermap: Statistics on the distribution of detected threats by country for month*. https://cybermap.kaspersky.com/stats

[4] International Telecommunication Union. (2024). *Global cybersecurity index 2024*. https://b2n.ir/fn6748

[5] Sophos. (2024). *The state of ransomware in financial services 2024*. https://news.sophos.com/en-us/2024/06/24/the-state-of-ransomware-in-financial-services-2024/

[6] Alghazo, J. M., Kazmi, Z., & Latif, G. (2017). Cyber security analysis of internet banking in emerging countries: user and bank perspectives. *2017 4th IEEE international conference on engineering technologies and applied sciences (ICETAS)* (pp. 1–6). IEEE. http://dx.doi.org/10.1109/ICETAS.2017.8277910

[7] Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of xidian university*, *14*(7), 1523–1536. https://www.researchgate.net/publication/337086201

[8] Sousa, R. D., Boranbayeva, A., Satpayeva, Z., & Gassanova, A. (2021). Management of successful technology transfer in agriculture: The case of Kazakhstan. *Problems and perspectives in management*, *19*(3), 488–501. http://dx.doi.org/10.21511/ppm.19(3).2021.40

[9] Akman, M. K. (2019). SWOT analysis and security management. *European journal of management and marketing studies*, *4*(2), 78–89. http://dx.doi.org/10.46827/ejmms.v0i0.624

[10] Yaşar, Ş. (2024). Integration of artificial intelligence in management accounting: A SWOT Analysis. *Journal of business in the digital age*, *7*(1), 9–19. http://dx.doi.org/10.46238/jobda.1474352

[11] Humphreys, E. (2016). *Implementing the ISO/IEC 27001: 2013 ISMS standard*. Artech house. https://books.google.com/books/about/Implementing_the_ISO_IEC_27001_2013_ISMS.html?id=Yy6pCwAAQBAJ

[12] Möller, D. P. F. (2023). NIST cybersecurity framework and MITRE cybersecurity criteria. In *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices* (pp. 231–271). Springer. https://doi.org/10.1007/978-3-031-26845-8_5

[13] Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23–40. http://dx.doi.org/10.1080/00396338.2011.555586

[14] Grothoff, C., & Moser, T. (2021). *How to issue a privacy-preserving central bank digital currency*. http://dx.doi.org/10.2139/ssrn.3965050

[15] Albrecht, J. P. (2016). How the GDPR will change the world. European data protection law review, *2*, 287. https://doi.org/10.21552/EDPL%2F2016%2F3%2F4

[16] Sunduk, T., Fadyeyeva, I., Yatsenko, O., & Pitel, N. (2024). Innovations and technological development in the financial sector of Ukraine: SWOT analysis and comparison of opportunities. *Futurity economics&law*, *4*(1), 52–63. https://doi.org/10.57125/FEL.2024.03.25.04