ECONOMIC SCIENCES

CYBERSECURITY IN FINANCIAL MARKETS: CURRENT STATE, RISKS, AND STRATEGIC CHALLENGES

Mammadov Y.
Doctor of Sciences in Economics, D.Sc. (Economics),
Institute of Economics of the Ministry of Science and Education of the Azerbaijan Republic,
Baku, Azerbaijan
https://doi.org/10.5281/zenodo.21411815

Abstract

The rapid digitalization of financial markets has elevated cyber risks to a core systemic threat, placing the impact of cyberattacks on financial stability at the forefront of the global regulatory agenda. However, a significant research gap remains regarding the cybersecurity landscape of financial markets in developing economies, including Azerbaijan. This study provides a comprehensive analysis of the current state of cybersecurity in the financial sector, examining attack typologies, international regulatory mechanisms, and global trends from 2020 to 2025 to derive strategic recommendations for Azerbaijan. Employing a mixed-methods approach—including quantitative-qualitative analysis, comparative country assessments, and a systematic literature review—this research utilizes empirical data from the IMF, ENISA, IBM Security, the World Economic Forum, and the BIS. The findings reveal that the financial sector accounted for 20% of all global cyber incidents in 2024, with the average cost of a data breach reaching USD 6.08 million 22% above the global cross-industry average. Ransomware, data breaches, AI-driven social engineering, and supply chain vulnerabilities constitute the primary risk categories. While international frameworks like the EU's DORA, US NIST standards, and the FS-ISAC model offer robust pathways for enhancing resilience, Azerbaijan requires tailored interventions. Consequently, this study recommends establishing a unified national cybersecurity coordination platform, deploying AI-based real-time monitoring systems, integrating mandatory stress-testing mechanisms into the regulatory framework, and accelerating human capital development within the financial sector.

Keywords: cybersecurity, financial markets, cyber risk, digital transformation, financial stability, artificial intelligence, regulatory frameworks, Azerbaijan.

Introduction

The digital transformation of the global economy has fundamentally altered the operational paradigms of financial markets in the contemporary era. Advances in information and communication technologies (ICT), the expansion of electronic commerce, the mass adoption of digital payment systems, and the proliferation of online financial service platforms have generated unprecedented opportunities for the sector. However, alongside these advancements, financial markets have increasingly become primary targets for sophisticated cybersecurity threats. The escalating frequency and complexity of cyberattacks targeting financial institutions, payment systems, and capital markets in recent years underscore the urgent need for systematic research in this domain [34].

The digital transformation of financial markets has accelerated significantly over the past decade. Digital banking, mobile payment systems, electronic wallets, open banking platforms, cloud computing, and AI-driven financial services have become foundational components of the sector. Notably, the proliferation of FinTech enterprises has not only enhanced the velocity and accessibility of financial transactions but has also fundamentally reshaped the cyber risk landscape. Consequently, the escalating reliance of financial systems on digital infrastructure has intensified systemic vulnerabilities, rendering the sector more susceptible to digital threats [20].

Cybersecurity plays a pivotal role in safeguarding financial stability, as cyberattacks targeting financial institutions can inflict severe repercussions not merely on individual firms, but on the systemic integrity of the financial architecture and the confidence of market participants. Prototypical threats—such as data breaches, the disruption of electronic payment systems, ransomware, and denial-of-service attacks—not only heighten operational risk but also serve as catalysts for systemic financial crises. Consequently, cybersecurity should transcend its traditional classification as a purely technical matter, being repositioned instead as a strategic dimension of financial stability, macro-economic security, and sustainable development [10]. The accelerating trajectory of digital transformation within the financial sector of Azerbaijan has concurrently brought these cybersecurity challenges to the forefront. The expanding volume of digital payments, the proliferation of internet and mobile banking services, and the growth of e-commerce collectively expose the sector to emerging categories of risk. While the Cybersecurity Strategy for Financial Markets for 2023–2026, formulated by the Central Bank of the Republic of Azerbaijan, establishes a robust institutional framework, the rapid pace of technological evolution necessitates its continuous iteration [5].

The primary objective of this study is to critically evaluate the contemporary state of cybersecurity in financial markets, delineate existing structural vulnerabilities, examine international regulatory frameworks, and formulate actionable policy recommendations tailored to Azerbaijan. To achieve this overarching aim, the following specific objectives have been established:

to analyze current trends in the digitalization of financial markets; to map the prevailing cyber-threat landscape within the financial sector; to quantify the impact of cybersecurity on financial stability; to execute a comparative analysis of international regulatory mechanisms; and to synthesize scientifically grounded, practice-oriented recommendations for Azerbaijan."

Literature Review

The foundational macroeconomic analysis of cybersecurity challenges within financial markets originates from the seminal study conducted by Kopp, Kaffenberger, and Wilson for the IMF [23]. The authors conceptualized cyber risk not merely as a technological anomaly, but as an economic risk capable of inducing market failures, demonstrating that capital allocations by financial institutions toward cybersecurity systematically fall short of the socially optimal threshold. This framework established the conceptual groundwork for integrating cyber risk into the broader paradigm of systemic financial risk. The International Monetary Fund has consistently reinforced this position in its subsequent literature. Notably, the IMF's 2024 Global Financial Stability Report highlighted the exponential increase in cyber incidents targeting financial institutions, emphasizing that the escalating interconnectedness of contemporary financial networks amplifies the risk of cross-institutional contagion [19].

From a microeconomic perspective, Gordon, Loeb, and Zhou examined the firm-level implications of information security breaches. Their empirical findings indicate that direct financial losses constitute merely a fraction of the total economic damage; conversely, reputational degradation, declines in market capitalization, erosion of consumer trust, and consequential legal liabilities represent the predominant share of the aggregate economic impact [16].

Corroborating this view, Romanosky independently concluded that governance frameworks and strategic management systems exert a more critical influence on risk mitigation than isolated technical defense mechanisms [30].

Regarding sector-specific dynamics in banking, the analysis compiled by Aldasoro, Gambacorta, Giudici, and Leach for the BIS merits particular attention. Their study identified a positive correlation between bank size and cyber risk exposure, while concurrently demonstrating that, unlike credit or market risks, cyber risk exhibits significantly lower statistical predictability [1].

Concurrently, ENISA's Threat Landscape reports dedicated to the financial sector provide a robust empirical foundation. According to these assessments, phishing campaigns, ransomware, social engineering, data breaches, and DDoS attacks account for the vast majority of sector-specific incidents; furthermore, a substantial proportion of these breaches is attributable to human factors rather than inherent technical vulnerabilities [11].

In the domain of capital markets, IOSCO's research underscores the vulnerability of trading platforms, clearing houses, and settlement systems to cyber disruptions, delineating how cyber incidents in securities markets adversely affect market liquidity, price discovery mechanisms, and investor behavior [21]. The cyber-resilience guidelines jointly formulated by CPMI and IOSCO have established a benchmark international regulatory reference point in this regard; this framework operationalizes cyber resilience not merely through prevention capabilities, but through the capacity to detect, respond to, and recover from operational disruptions [6].

Concerning FinTech architectures, reports from the World Economic Forum indicate that open banking APIs, cloud-based configurations, and artificial intelligence models have introduced novel risk vectors, thereby elevating third-party risk to the core of regulatory oversight [34].

Biener, Eling, and Wirfs elucidated the challenges of underwriting cyber risks through traditional insurance models, demonstrating that these risks constitute an anomalous category due to their extreme uncertainty and systemic nature [3]. Research executed by the US Federal Reserve on the macroeconomic repercussions of cyber risk similarly validates that attacks targeting systemic nodes can trigger widespread financial contagion. Furthermore, a report by the Carnegie Endowment for International Peace underscores the imperative of strengthening multilateral cooperation mechanisms to counter cyber threats to the global financial architecture [4].

A critical synthesis of the existing literature reveals that, while researchers universally acknowledge the strategic salience of cybersecurity for financial stability, several structural gaps persist [7]. Primarily, contemporary literature is heavily concentrated on the financial ecosystems of advanced economies—specifically the United States, the United Kingdom, and the European Union [33]. Furthermore, the banking sector, capital markets, payment infrastructures, and FinTech platforms are predominantly analyzed in isolation, resulting in insufficient exploration of their systemic interdependencies [9]. Empirical investigations assessing the cybersecurity posture within the financial markets of developing economies, including Azerbaijan, remain remarkably scarce. Rectifying this empirical deficit is essential from both a theoretical and a policy-oriented standpoint.

Cybersecurity Posture and Regulatory Mechanisms in Financial Markets:

International Practice

The pervasive digital transformation of the global financial architecture has exponentially heightened systemic cybersecurity risks. Over the past decade, the widespread proliferation of Omni channel banking ecosystems, electronic payment infrastructures, digital investment platforms, and FinTech architectures has fundamentally intensified the financial sector's structural reliance on information technology networks. According to empirical estimates by the IMF, direct financial losses stemming from systemic cyber incidents within the financial sector over the trailing two decades have surpassed 12 billion US dollars, with cumulative indirect economic repercussions and institutional reputational degradation amplifying this aggregate figure multi-fold [20]. Correspondingly, research by the BIS on the evolution of the FinTech sector validates that digital transformation introduces not only operational efficiencies but also novel supervisory burdens for

macroprudential banking oversight [2]. Furthermore, a World Bank assessment indicates that balancing the expansion of financial inclusion with the preservation of robust cybersecurity frameworks presents a critical policy trilemma for developing economies [33]. The empirical matrix below delineates a comparative analysis of cybersecurity preparedness across selected jurisdictions.

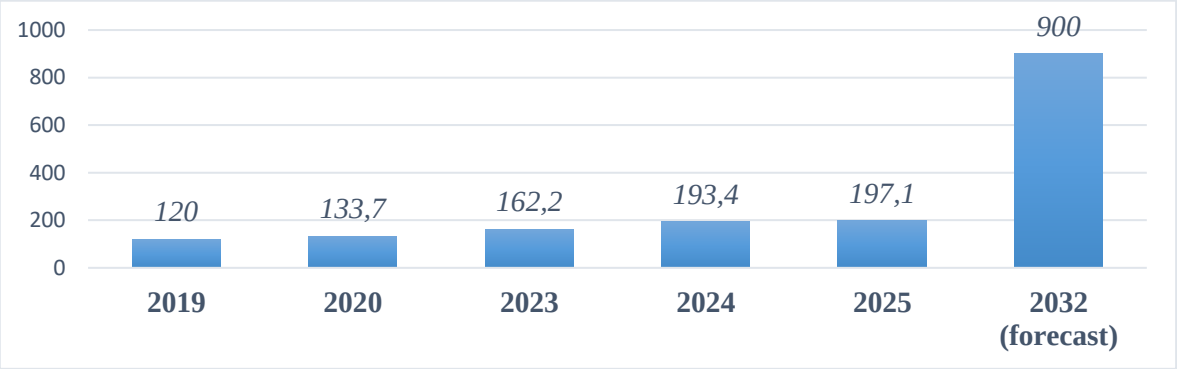

Figure 1. The volume of the global cybersecurity market in recent years (billion USD)
Source: https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

The analysis conducted shows that a significant increase has been observed in the volume of the global cybersecurity market in recent years. For instance, while the total market volume in this field was 120 billion USD in 2019, this figure increased to 193.4 billion USD in 2024 and reached 248.28 billion USD in 2026. According to the economic analyses conducted, this indicator is projected to rise to 699.39 billion USD in 2034 (Figure 1).

Table 1.

Comparative Indicators of Cybersecurity Posture by Selected Jurisdiction (2024)

Country	GCI Index	NCSI Index	Share of Cyberattacks in Financial Sector (%)
United States	100	94.8	22
United Kingdom	99.5	92.2	19
Singapore	99.8	91.4	17
Germany	98.7	89.6	18
Estonia	98.1	100	14

Source: Compiled by the author based on [22]; [26].

As delineated in Table 1, jurisdictions exhibiting advanced cybersecurity postures concurrently lead the development of digital financial services (Table 1). This positive correlation implies that sustaining the socio-economic dividends generated by digital transformation necessitates the synchronized evolution of cybersecurity frameworks. Absent such alignment, cyber disruptions targeting the core digital infrastructure of the financial architecture may function as a primary transmission mechanism for systemic risk. Concurrently, the structural composition of international cyber threats targeting the financial sector has undergone a paradigm shift over recent years [34]. Although data breaches aimed at expropriating personal information historically predominated, operational disruptions designed to compromise the systemic functionality of financial networks have increasingly migrated to the forefront [8].

Table 2.

Structural Composition of Primary Cyber Threats within the Financial Sector (2024)

Type of Cyber Threat	Share of Total Incidents (%)
Ransomware attacks	35
Data theft and breaches	27
Social engineering (phishing)	18
DDoS attacks	12
Supply chain attacks	8

Source: Compiled by the author based on [8]; [17].

As illustrated in Table 2, the most pervasive risk vector within the financial sector is attributable to ransomware campaigns (Table 2). The primary objective of these exploits is to extract financial leverage by freezing or severely disrupting the operational continuity of financial institutions. Furthermore, the escalating structural reliance on third-party service providers introduces critical systemic vulnerabilities, thereby facilitating the propagation of these risks [12]. To mitigate these threats, robust regulatory frameworks have been formulated at the international level to fortify organizational cyber resilience. The Digital Operational Resilience Act (DORA), enacted by the European Union in 2022, mandates stringent obligations for financial institutions concerning cyber risk management, incident disclosure protocols, mandatory resilience stress testing [27], and the oversight of third-party dependencies. In the United States, the NIST Cybersecurity Framework 2.0 and the FS-ISAC operational model serve as the premier benchmarks for sector-specific risk mitigation

[13]. Concurrently, the Financial Stability Board's recommendations on cyber incident reporting function as a cornerstone strategic document aimed at enhancing multilateral coordination [14]. Similarly, the Technology Risk Management Guidelines enforced by the Monetary Authority of Singapore (MAS) have played a pivotal role in establishing unified cybersecurity standards across the Asia-Pacific financial architecture [25].

Concurrently, the COVID-19 pandemic catalyzed a mass migration of banking and payment infrastructures to digital channels, significantly expanding the financial sector's threat surface [20]. Empirical estimates by the IMF indicate that the frequency of cyberattacks approximately doubled post-2020 relative to the pre-pandemic baseline, with roughly twenty percent of globally documented cyber incidents targeting financial entities. The empirical matrix in Table 3 delineates the trajectory of key indicators during this timeframe [26].

Table 3.

Major Cybersecurity Trends in the Financial Sector (2020–2025)

Indicator	2020–2021	2022–2023	2024	2025
Share of financial sector (total incidents)	~15%	~18%	~20%	~20%+
Global average cost of a data breach (USD mln)	3.86 / 4.24	4.35 / 4.45	4.88	4.44
Average cost in financial sector (USD mln)	~5.0+	High	6.08	~5.56
Ransomware encryption rate	Rising	Continuing	70%	50%
AI-driven social engineering	Early stage	Rising	Expanding	High risk

Source: Compiled by the author based on [17]; [18]; [31]; [34].

"According to IBM Security's 2024 report, the global average financial impact of a single data breach reached 4.88 million US dollars, whereas within the financial sector, this metric escalated to 6.08 million US dollars—marking a 22% premium over the global baseline [17]. Although the subsequent contraction of the global average to 4.44 million US dollars in 2025 indicated a heightened efficacy in AI-driven detection mechanisms, the financial sector concurrently maintained its classification as a critically high-risk domain [18]."

Table 4.

Comparison of Average Data Breach Costs, 2020–2025 (USD million)

Year	Global Average	Financial Sector	Key Notes
2020	3.86	~5.0+	Pandemic-era risks
2021	4.24	High	Hybrid work models
2022	4.35	High	Supply chain attacks
2023	4.45	High	Rising compliance costs
2024	4.88	6.08	Financial sector 22% above average
2025	4.44	~5.56	AI detection shortened response time; sector still high-risk

Source: Compiled by the author based on [17]; [18].

"According to Sophos's 2025 report, the encryption efficacy rate within ransomware campaigns declined from 70% in 2024 to 50% in 2025 [31]. Although this contraction reflects advancements in robust defense frameworks, it does not imply a mitigation of the overall ransomware threat landscape (Table 4). Over this period, threat actors systematically pivoted from traditional encryption protocols toward data exfiltration, double-extortion architectures, and reputational leverage tactics [30].

Concurrently, the World Economic Forum's 2025 report underscores that generative artificial intelligence has augmented the sophistication, cost-efficiency, and scalability of phishing, vishing, deepfake, and social engineering exploits. This technological evolution poses an existential vulnerability for the financial sector, wherein core operational pillars—such as banking transactions, KYC (Know Your Customer) identification protocols, and payment authorization mechanisms—are structurally predicated on institutional trust. Regarding capital allocation, global cybersecurity expenditures expanded from approximately 260 billion US dollars in 2021 to 454 billion US dollars in 2025 [35]. Ultimately, given that aggregate global annualized cyber losses reached an estimated 10.5 trillion US dollars by 2025, it is evident that cyber risk has permanently transitioned into a critical macroeconomic hazard. (Table 5)

Table 5.

Key Indicators of Cybersecurity Spending and AI-Related Risks

Indicator	2020–2021	2024	2025
Global cybersecurity spending	$260 billion	Continued growth	$454 billion
Projected global annual cyber losses	Growth phase	Trillions	$10.5 trillion
AI-driven social engineering	Limited	GenAI phishing	Deepfake, vishing
Defense model in financial sector	Traditional	Risk monitoring	AI analytics

Source: Compiled by the author based on [35]; [15].

Mitigating Cybersecurity Risks in Financial Markets via AI-Driven Solutions

As the digital transformation of financial markets accelerates, conventional cybersecurity mechanisms exhibit diminishing efficacy in countering sophisticated contemporary exploits. Within this paradigm, embedding innovative architectures—specifically artificial intelligence—into the defensive infrastructure of the financial sector has emerged as a strategic imperative [1]. By executing real-time behavioral analytics, AI-driven technologies possess the capability to identify emerging threat vectors that legacy signature-based systems fail to detect (Table 6). According to empirical findings by Deloitte, the deployment of cognitive technologies has compressed the mean time to detect (MTTD) security incidents in financial institutions by 40% to 60% [34].

Table 6.

Key Applications of AI-Based Cybersecurity Solutions in the Financial Sector

Area of Application	Main Objective	Expected Outcome
Fraud detection	Identifying suspicious transactions	Reduction in financial losses
Behavioral analytics	Detecting anomalous activity	Early-warning capability
Real-time risk monitoring	Dynamic risk tracking	Faster decision-making
Automated response systems	Rapid reaction to attacks	40–60% reduction in response time
Biometric authentication	User identity verification	Strengthened account security

Source: Compiled by the author based on [28]; [8].

"Global payment conglomerates, such as Visa and Mastercard, systematically leverage AI-driven architectures [32]. to process and analyze multi-million transaction streams daily, thereby mitigating potential risk vectors in real time. Concurrently, blockchain technology is increasingly recognized as a viable complementary framework; by introducing immutable ledger systems that impede data tampering, it enhances transactional transparency and curtails fraudulent exploits [24]. Accounting for the idiosyncratic characteristics of Azerbaijan's digital financial ecosystem, the operationalization of the following five strategic pillars carries paramount significance:

- Strategic Pillar I: Institutionalization of a Unified Cyber-Resilience Coordination Platform. Inter-institutional information sharing across the national financial sector is currently constrained [20]. Establishing a national financial cybersecurity infrastructure modeled after the global FS-ISAC framework would fortify cross-sectoral synergy and proactive threat intelligence sharing [29].
- Strategic Pillar II: Pervasive Deployment of Cognitive Monitoring Architectures. Within the banking sector, the institutionalization of AI-driven real-time behavioral diagnostics, automated anomaly detection, and algorithmic fraud mitigation would substantially elevate the aggregate cybersecurity posture.
- Strategic Pillar III: Implementation of Mandatory Cyber-Resilience Stress Testing Frameworks. Adopting international benchmarks—specifically the European Union's DORA framework—enables the empirical evaluation of systemic resilience under simulated crisis conditions [18]. Consequently, the Central Bank of Azerbaijan should mandate comparable macroprudential regulatory stress-testing requirements for systemically important financial institutions (SIFIs).
- Strategic Pillar IV: Optimization and Cultivation of Human Capital. Empirical evidence demonstrates that a critical proportion of cyber breaches originates from human errors rather than inherent infrastructure vulnerabilities. Accordingly, embedding a comprehensive cybersecurity governance culture within financial entities, supported by continuous pedagogical training, is essential to minimize operational risk vectors [9].
- Strategic Pillar V [2]: Advanced Risk Governance of Third-Party Dependencies. As the integration of FinTech architectures accelerates, the continuous mapping, assessment, and oversight of risk transmission channels introduced by external vendor networks and third-party service providers remain vital for systemic stability .

Conclusion

This study has provided a comprehensive investigation into the contemporary posture of cybersecurity within financial markets, delineating prevalent global trajectories and formulating strategic dimensions tailored to the Azerbaijani context. The critical synthesis of the empirical and qualitative findings yields several pivotal conclusions.

Primarily, the analysis confirms that cybersecurity has transcended its traditional classification as an isolated technical issue, emerging instead as a foundational strategic determinant of macroeconomic financial stability. Direct capital losses stemming from systemic cyber incidents within the global financial architecture have surpassed 12 billion US dollars over the trailing decade. Furthermore, the empirical evidence that the mean financial impact of a data breach within the financial domain in 2024 (6.08 million US dollars) exhibited a 22% premium over the global baseline validates that this sector possesses an inherently distinct and elevated risk profile.

Secondly, the structural composition of the cyber-threat landscape has undergone a significant paradigm shift. A highly sophisticated defense challenge has materialized, characterized by the convergence of ransomware campaigns, data breaches, AI-driven social engineering exploits, and supply-chain vulnerabilities. The proliferation of generative artificial intelligence models has markedly optimized the cost-efficiency and scalability of executing malicious campaigns, thereby intensifying systemic fragility.

Thirdly, the comparative evaluation of international regulatory practices demonstrates that robust cyber-resilience frameworks cannot rely exclusively on

technological deployment; rather, they must encompass tightly integrated regulatory, institutional, and human-capital dimensions. Frameworks such as the European Union's DORA, the NIST Cybersecurity Framework, the global FS-ISAC model, and the MAS Technology Risk Management Guidelines stand as premier benchmarks that effectively institutionalize this multi-dimensional coordination requirement.

For the digital economy of Azerbaijan, these findings carry profound policy and practical implications [17]. While the Cybersecurity Strategy for Financial Markets for 2023–2026, formulated by the Central Bank of Azerbaijan, establishes an important institutional foundation, the rapidly evolving digital ecosystem necessitates the continuous iteration of this framework. This includes the integration of cognitive AI-driven defense mechanisms, the institutionalization of intra-sectoral threat intelligence sharing platforms, and enhanced capital allocation toward human capital development. Finally, a recognized limitation of this study is the empirical scarcity of localized, sector-specific cyber incident statistics within Azerbaijan. Consequently, future research trajectories should be predicated on direct empirical surveys and quantitative incident analysis executed in closer alignment with local financial institutions.

References:

1. Aldasoro I., Gambacorta L., Giudici P., Leach T. Operational and Cyber Risk in the Financial Sector // BIS Working Papers No. 1005. — Basel: Bank for International Settlements, 2022. — URL: https://www.bis.org/publ/work1005.htm (accessed: 01.06.2026).

2. Bank for International Settlements (BIS). Sound Practices: Implications of FinTech Developments for Banks and Bank Supervisors. — Basel: BIS, 2021. — URL: https://www.bis.org/bcbs/publ/d431.htm (accessed: 01.06.2026).

3. Biener C., Eling M., Wirfs J.H. Insurability of Cyber Risk: An Empirical Analysis // The Geneva Papers on Risk and Insurance – Issues and Practice. — 2015. — Vol. 40, No. 1. — P. 131–158. DOI: 10.1057/gpp.2014.19.

4. Carnegie Endowment for International Peace. International Strategy to Better Protect the Financial System against Cyber Threats. — Washington, DC: Carnegie Endowment, 2020. — URL: https://carnegieendowment.org/research/2020/11/international-strategy-to-better-protect-the-financial-system-against-cyber-threats (accessed: 01.06.2026).

5. Central Bank of the Republic of Azerbaijan. Cybersecurity Strategy for Financial Markets (2023–2026). — Baku: CBAR, 2023. — URL: https://uploads.cbar.az/assets/9018b71b0859bc7a490ea0f22.pdf (accessed: 01.06.2026).

6. Committee on Payments and Market Infrastructures (CPMI), International Organization of Securities Commissions (IOSCO). Guidance on Cyber Resilience for Financial Market Infrastructures. — Basel: Bank for International Settlements, 2016. — URL: https://www.bis.org/cpmi/publ/d146.pdf (accessed: 01.06.2026).

7. Cybersecurity Ventures. Cybersecurity Market Report 2025–2026. — Northport, NY: Cybersecurity Ventures, 2025. — URL: https://cybersecurityventures.com (accessed: 01.06.2026).

8. Deloitte. Financial Services Industry Cybersecurity Outlook 2024. — London: Deloitte, 2024. — URL: https://www2.deloitte.com/global/en/pages/financial-services/articles/cybersecurity-financial-services.html (accessed: 01.06.2026).

9. Eisenbach T.M., Kovner A., Lee M.J. Cyber Risk and the U.S. Financial System // Federal Reserve Bank of New York Staff Reports, No. 1014. — New York: FRBNY, 2022. — URL: https://www.newyorkfed.org/research/staff_reports/sr1014 (accessed: 01.06.2026).

10. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. — Athens: ENISA, 2024. — URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (accessed: 01.06.2026).

11. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape: Finance Sector. — Athens: ENISA, 2024. — URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector (accessed: 01.06.2026).

12. European Union. Regulation (EU) 2022/2554 of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector (DORA) // Official Journal of the European Union. — 2022. — L 333. — P. 1–79. — URL: europa.eu (accessed: 01.06.2026).

13. Financial Services Information Sharing and Analysis Center (FS-ISAC). Annual Global Intelligence Report 2025. — Herndon, VA: FS-ISAC, 2025. — URL: https://www.fsisac.com (accessed: 01.06.2026).

14. Financial Stability Board (FSB). Recommendations to Achieve Greater Convergence in Cyber Incident Reporting. — Basel: FSB, 2023. — URL: https://www.fsb.org/2023/04/recommendations-to-achieve-greater-convergence-in-cyber-incident-reporting-final-report (accessed: 01.06.2026).

15. FS-ISAC. Navigating Cyber 2025: Financial Services Threats and Trends. — Herndon, VA: Financial Services Information Sharing and Analysis Center, 2025. — URL: https://www.fsisac.com (accessed: 01.06.2026).

16. Gordon L.A., Loeb M.P., Zhou L. The impact of information security breaches: Has there been a downward shift in costs? // Journal of Computer Security. — 2011. — Vol. 19, No. 1. — P. 33–56. DOI: 10.3233/JCS-2010-0398.

17. IBM Security. Cost of a Data Breach Report 2024. — Armonk, NY: IBM Corporation, 2024. URL: https://www.ibm.com/reports/data-breach (accessed: 01.06.2026).

18. IBM Security. Cost of a Data Breach Report 2025. — Armonk, NY: IBM Corporation, 2025. URL: https://www.ibm.com/reports/data-breach (accessed: 01.06.2026).

19. International Monetary Fund. Cyber Risk: A Growing Concern for Macrofinancial Stability // Global Financial Stability Report, April 2024, Chapter 3. — Washington, DC: IMF, 2024. — URL:

https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024 (accessed: 01.06.2026).

20. International Monetary Fund. Global Financial Stability Report: The Last Mile — Financial Vulnerabilities and Risks. — Washington, DC: IMF, 2024. — URL: https://www.imf.org/en/Publications/GFSR (accessed: 01.06.2026).

21. International Organization of Securities Commissions (IOSCO). Cyber Crime, Securities Markets and Systemic Risk. — Madrid: IOSCO, 2016. — URL: https://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf (accessed: 01.06.2026).

22. International Telecommunication Union (ITU). Global Cybersecurity Index 2024. — Geneva: ITU, 2024. — URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed: 01.06.2026).

23. Kopp E., Kaffenberger L., Wilson C. Cyber Risk, Market Failures, and Financial Stability // IMF Working Paper No. 17/185. — Washington, DC: International Monetary Fund, 2017. — URL: https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104 (accessed: 01.06.2026).

24. Mastercard. Cyber and Intelligence Solutions Report 2024. — Purchase, NY: Mastercard, 2024.

25. Monetary Authority of Singapore (MAS). Technology Risk Management Guidelines. — Singapore: MAS, 2023. — URL: https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines (accessed: 01.06.2026).

26. National Cyber Security Index (NCSI). NCSI Database 2024. — Tallinn: e-Governance Academy, 2024. — URL: https://ncsi.ega.ee (accessed: 01.06.2026).

27. National Institute of Standards and Technology (NIST). Artificial Intelligence Risk Management Framework (AI RMF 1.0). — Gaithersburg, MD: NIST, 2024. — URL: https://www.nist.gov/system/files/documents/2023/01/26/AI%20RMF%201.0.pdf (accessed: 01.06.2026).

28. National Institute of Standards and Technology (NIST). Cybersecurity Framework 2.0. — Gaithersburg, MD: NIST, 2024. — URL: https://www.nist.gov/cyberframework (accessed: 01.06.2026).

29. Organisation for Economic Co-operation and Development (OECD). Digital Finance and Blockchain Technologies. — Paris: OECD Publishing, 2024. — URL: https://www.oecd.org/finance/digital-finance-and-blockchain.htm (accessed: 01.06.2026).

30. Romanosky S. Examining the costs and causes of cyber incidents // Journal of Cybersecurity. — 2016. — Vol. 2, No. 2. — P. 121–135. DOI: 10.1093/cybsec/tyw001.

31. Sophos. The State of Ransomware 2025. — Oxford: Sophos, 2025. — URL: https://www.sophos.com/en-us/whitepaper/state-of-ransomware (accessed: 01.06.2026).

32. Visa Inc. Annual Risk and Security Report 2024. — Foster City, CA: Visa Inc., 2024.

33. World Bank. Cybersecurity and Financial Consumer Protection in Digital Finance. — Washington, DC: World Bank, 2022. — URL: https://documents.worldbank.org (accessed: 01.06.2026).

34. World Economic Forum. Global Cybersecurity Outlook 2024. — Geneva: WEF, 2024. — URL: https://www.weforum.org/reports/global-cybersecurity-outlook-2024 (accessed: 01.06.2026).

35. World Economic Forum. Global Cybersecurity Outlook 2025. — Geneva: WEF, 2025. — URL: https://www.weforum.org/reports/global-cybersecurity-outlook-2025 (accessed: 01.06.2026).