

## CYBERSECURITY AND SECURE COMMUNICATION CHANNELS AS STRATEGIC ENABLERS OF DIGITAL TRANSFORMATION AND RISK GOVERNANCE IN THE FINANCIAL SECTOR

Pawel Frankiewicz<sup>1</sup>, Serhii Zahranynychnyi<sup>2</sup>

<sup>1</sup> PhD in Law, Chief Executive Officer of the European Economic Society LLC, Jarosław, Poland

Email: pawelfrankiewich@gmail.com, ORCID: <https://orcid.org/0009-0002-8816-7376>

<sup>2</sup> M.Sc. in Software Engineering for Automated Systems, Principal Associate, Risk Tech Department, Capital One Financial Corporation, Tysons Corner, Virginia, United States

Email: zagranlab@gmail.com, ORCID: <https://orcid.org/0009-0001-1867-0323>

**ABSTRACT.** The financial sector's digital transformation has significantly increased institutional dependence on information and communication technologies, third-party digital infrastructures, and real-time data exchange. In this environment, cybersecurity can no longer be treated as a narrowly technical or auxiliary IT function. This article argues that cybersecurity and secure communication channels should be understood as strategic enablers of digital transformation and integral components of risk governance in the financial sector. The study employs a conceptual, regulatory-analytical, and literature-synthesis approach grounded in contemporary international and European frameworks on digital operational resilience, cyber risk supervision, and incident response, while also drawing on the scholarly literature on cybersecurity governance and financial cybersecurity risk management. It shows, on the basis of reviewed frameworks and literature, that cybersecurity and secure communications underpin institutional resilience, regulatory compliance, operational continuity, crisis coordination, and stakeholder trust. It further argues that secure communication channels perform a governance function by enabling escalation, decision-making, recovery coordination, and communication with regulators and counterparties during disruptive events. The article concludes that in digitally transformed finance, cybersecurity and secure communication channels should be treated not as peripheral technical safeguards but as structural elements of resilience-oriented risk governance.

**Keywords:** *cybersecurity; secure communication channels; digital transformation; risk governance; financial sector; digital operational resilience; information and communication technology (ICT); risks; cyber resilience; operational resilience; financial regulation.*

### INTRODUCTION

Digital transformation has become one of the defining structural processes of the contemporary financial sector. Financial institutions increasingly rely on interconnected ICT infrastructures, cloud-based services, outsourced digital functions, and real-time information flows to deliver payments, investment services, lending operations, reporting, and customer interaction. At the same time, this transformation has expanded the sector's exposure to cyber risk, operational disruption, and complex interdependencies involving both internal systems and third-party providers. In the European Union, this growing dependence on ICT is reflected in Regulation (EU) 2022/2554, the Digital Operational Resilience Act (DORA), which establishes a harmonized framework for the management of ICT-related risk in the financial sector [5].

Against this background, cybersecurity can no longer be interpreted as a purely technical layer of institutional defence. Contemporary regulatory and supervisory frameworks increasingly treat cyber resilience, ICT risk management, incident response, recovery capability, and operational continuity as core components of financial-sector governance. Similar logic is reflected in the Basel Committee's principles for operational resilience, the Financial Stability Board's work on cyber

---

incident response and recovery, the ECB's cyber resilience oversight expectations, and NIST CSF 2.0, which explicitly places governance at the core of cybersecurity risk management [1; 4; 6; 10].

At the same time, an important governance problem remains insufficiently conceptualized in both academic and practice-oriented discussion. Although financial institutions increasingly depend on secure and coordinated digital interaction, cybersecurity and secure communication channels are still too often treated as technical safeguards or procedural add-ons rather than as resilience-enabling mechanisms within the governance architecture of the financial sector. This is scientifically and practically significant, since the sustainability of digital transformation in finance depends not only on the protection of systems, but also on the institutional capacity to maintain secure coordination, trusted escalation, operational continuity, and effective response under conditions of cyber and operational disruption.

The **purpose of this article** is to develop a governance-oriented interpretation of cybersecurity and secure communication channels in the financial sector and to substantiate their role as strategic enablers of digital transformation and resilience-oriented risk governance. The article proceeds from the assumption that digital transformation in finance cannot be institutionally sustainable unless cybersecurity and secure communications are embedded into governance structures, resilience frameworks, and compliance architecture.

### **Research methodology**

This article adopts a conceptual, regulatory-analytical, and literature-synthesis design rather than an empirical case-study approach. It operates within a non-empirical scope and relies on analytical interpretation, conceptual integration, and structured engagement with authoritative regulatory, supervisory, and scholarly materials.

The evidentiary base consists of three complementary layers. First, the article draws on official regulatory and supervisory frameworks, including international and European materials on digital operational resilience, ICT risk, cyber incident response and recovery, and operational continuity. Second, it synthesizes selected scholarly literature on cybersecurity governance, financial-sector cyber risk management, cyber resilience, and communication in cyber-related organizational settings. Third, it incorporates sectoral analytical evidence from institutional reports and datasets in order to support the argument with data-based exhibits in addition to normative and conceptual reasoning.

Given this design, the article does not claim to establish causal relationships in an empirical sense. Instead, it advances an interpretive synthesis that identifies, organizes, and connects dispersed regulatory, conceptual, and analytical materials in order to clarify the governance significance of cybersecurity and secure communication channels in digitally transformed finance. Accordingly, the conclusions should be read as analytically substantiated and governance-relevant rather than as universally verified causal claims.

### **Literature Review and Research Gap**

The current literature does not form a single mature subfield explicitly organized around the proposition that secure communication channels are strategic enablers of digital transformation and risk governance in the financial sector. A more accurate reading is that the topic sits at the intersection of several established literatures: cybersecurity governance, financial cybersecurity risk management, cyber and operational resilience, regulation of ICT dependencies, and communication in cyber-incident settings. The contribution of the present article is therefore integrative: it connects these strands into a unified governance-oriented framework centered on the financial sector.

A first relevant line of scholarship concerns cybersecurity governance. Oh et al. (2025) present cybersecurity governance as a holistic organizational framework embedded within enterprise risk management and linked to broader corporate governance practices. A second line is financial cybersecurity risk management. Rohmeyer and Bayuk (2019) frame cybersecurity in financial systems through leadership, governance, institutional oversight, and risk management in

systems and institutions rather than as a purely engineering problem. Together, these works support the analytical move from “technical control” to “governance-enabling capability” [11; 13].

A third line concerns cyber resilience and operational resilience. Here the key move is from prevention alone toward preparedness, endurance through disruption, coordination, recovery, and adaptation. In the financial sector, this shift is particularly important because institutions operate through dense technological interdependencies, external service dependencies, and high continuity expectations. The regulatory and supervisory literature makes this logic especially clear: the Basel Committee links operational resilience with governance, continuity of critical operations, and dependency management; the FSB treats governance, planning, coordination, and communication as core components of cyber incident response and recovery; and the ECB places cyber resilience within the broader operational risk and continuity environment of financial market infrastructures [1; 4; 6].

A fourth line concerns the relationship between regulation and governance for cyber resilience. Cojocaru (2025) is especially important because it explicitly links regulation and governance in the cyber-resilience context of the financial sector. A fifth, narrower line concerns communication and discourse in cyber settings. Davis et al. (2025) examine how cybersecurity discourse in financial institutions can either align teams or divide them. This does not yet amount to a mature stand-alone subfield on secure communication channels as governance infrastructure, but it does provide scholarly support for treating communication as an organizational dimension of cyber resilience [2; 3].

The research gap is therefore not the total absence of work on cybersecurity, resilience, or communication. Rather, it is the insufficient integration of these literatures around the specific role of secure communication channels as a governance-relevant enabling mechanism in digitally transformed finance. This article addresses that gap by integrating official resilience frameworks with the emerging scholarly conversation on cybersecurity governance and financial cyber risk.

## **PRESENTATION OF THE MAIN RESEARCH MATERIAL**

### **Digital Transformation and the Expanding Risk Architecture of the Financial Sector**

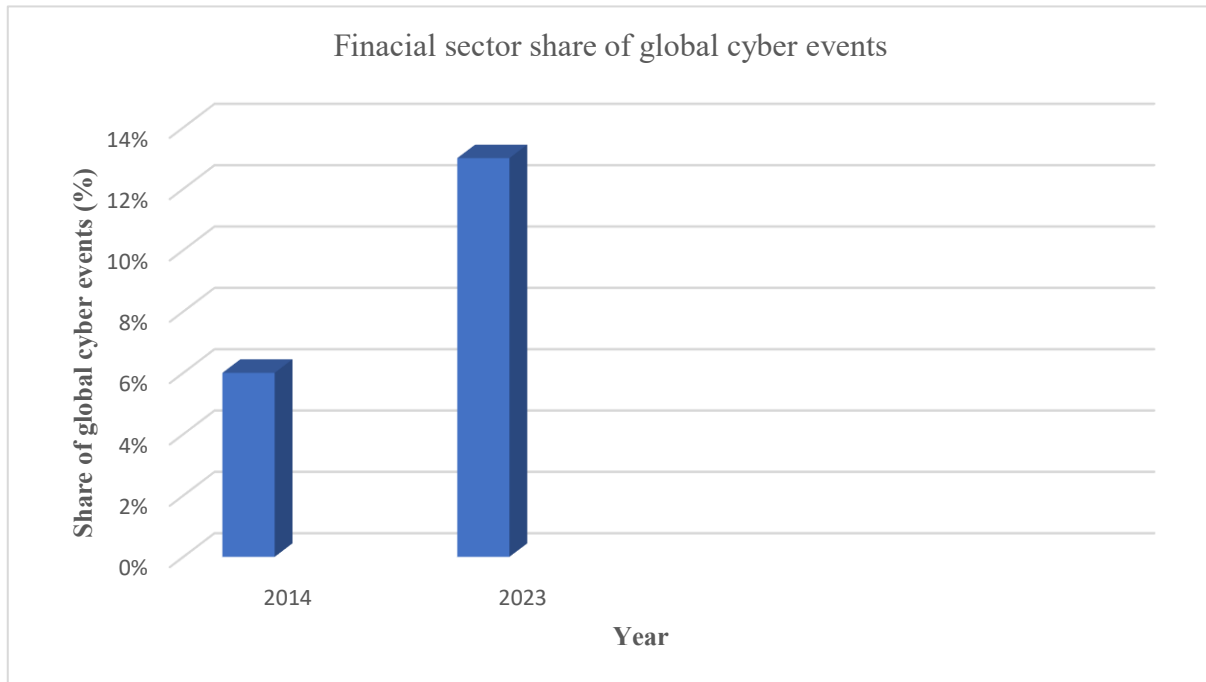
Digital transformation has become a structural feature of the contemporary financial sector. Financial institutions increasingly rely on interconnected ICT systems, cloud services, data-intensive processes, third-party providers, and real-time digital infrastructures. As digital transformation deepens, the risk architecture of the financial sector becomes broader and more interdependent. The relevant problem is no longer limited to isolated cyberattacks against single institutions. Financial entities are increasingly exposed to combinations of cyber risk, operational risk, concentration risk related to ICT third-party providers, incident propagation across interconnected systems, and disruptions that may impair the continuity of critical functions. DORA explicitly reflects this expanded risk architecture by covering ICT risk management, ICT-related incident reporting, digital operational resilience testing, ICT third-party risk, and information-sharing arrangements within a single framework [5].

The Basel Committee defines operational resilience in terms of the ability of a bank to deliver critical operations through disruption and emphasizes governance, operational risk management, business continuity, mapping of interdependencies, and scenario testing [1]. The Financial Stability Board’s effective practices similarly frame cyber incidents not only as technical failures but as events with operational, organizational, and potentially systemic consequences that require governance, planning, mitigation, restoration, and communication [6]. NIST CSF 2.0 reinforces this shift by placing “Govern” alongside Identify, Protect, Detect, Respond, and Recover [10].

The scholarly literature supports this widening of the analytical lens. Oh et al. (2025) frame cybersecurity governance as embedded in enterprise risk management, while Rohmeyer and Bayuk (2019) treat financial cybersecurity as a leadership and institutional issue. This suggests that digital transformation in finance should not be analyzed merely as a technology-adoption process. It

should also be understood as a process that expands institutional vulnerability surfaces and therefore expands governance responsibilities [11; 13].

The exposure of finance to cyber events is also visible in sectoral evidence. IMF analysis identified 14,055 distinct cyber events across 20 sectors and 162 jurisdictions, of which 1,246 were in the financial sector; the share of cyber events attributed to the financial sector rose from 6% in 2014 to 13% in 2023 [9]. This does not by itself prove causality between digital transformation and cyber exposure, but it provides strong analytical support for the claim that cyber risk has become structurally salient in finance. To make this sectoral shift more explicit, Figure 1 provides a concise visual representation of this sectoral trend.



**Figure 1. Increase in the Financial Sector's Share of Reported Global Cyber Events, 2014–2023**

*Note.* Prepared from IMF Working Paper data. The figure shows the increase in the financial sector's share of reported global cyber events from 6% in 2014 to 13% in 2023.

*Source:* Khiaonarong and Zheng (2026) [9].

As shown in Figure 1, the financial sector's share of reported global cyber events increased markedly over the period under review. While this trend does not by itself establish a direct causal relationship between digital transformation and cyber exposure, it provides strong sectoral evidence that cyber risk has become increasingly salient in finance and therefore more difficult to treat as a peripheral technical concern.

Taken together, these developments suggest that the central issue is no longer whether cybersecurity matters in finance, but how cybersecurity should be positioned within the strategic and governance architecture of digitally transformed financial institutions.

### **Cybersecurity as a Strategic Enabler Rather Than a Technical Add-On**

In the contemporary financial sector, cybersecurity can no longer be understood adequately as a narrowly technical function designed only to protect digital assets from unauthorized access or disruption. The increasing integration of financial services with ICT systems, cloud infrastructures, outsourced digital functions, and real-time transactional environments has transformed cybersecurity into a strategic condition for institutional viability. In this context, cybersecurity should be analyzed not as a peripheral support mechanism, but as an enabling infrastructure for digital transformation itself. This interpretation is consistent with DORA, which

requires financial entities to withstand, respond to, and recover from ICT-related disruptions and threats [5].

This governance-oriented interpretation is reinforced by scholarly literature. Oh et al. (2025) frame cybersecurity governance as a holistic framework embedded within enterprise risk management and broader governance structures. Rohmeyer and Bayuk (2019) likewise discuss financial cybersecurity risk management in leadership and institutional terms, linking cybersecurity with executive oversight, risk management, and sector-specific governance demands. Read together, these works support the proposition that cybersecurity should be interpreted as an enabling condition for digitally mediated institutional functioning rather than as a technical appendage to digital transformation [11; 13].

From the standpoint of risk governance, cybersecurity underpins institutional resilience, supports regulatory compliance, sustains trust among customers and market participants, and enables continuity of financial services. These functions explain why cybersecurity must be treated as governance-relevant infrastructure rather than as a merely technical safeguard.

### **Secure Communication Channels in Incident Response, Coordination, and Continuity**

In a digitally intensive financial environment, secure communication channels should be understood as institutional mechanisms that support the reliable transmission, escalation, verification, and coordination of information during routine operations and, especially, under conditions of disruption. Their significance becomes particularly visible during cyber incidents, when ordinary communication infrastructures may be degraded, compromised, unavailable, or no longer trustworthy. The Financial Stability Board explicitly treats coordination and communication as a distinct component of cyber incident response and recovery and considers scenarios in which ordinary communication channels may be unavailable during a cyber incident [6].

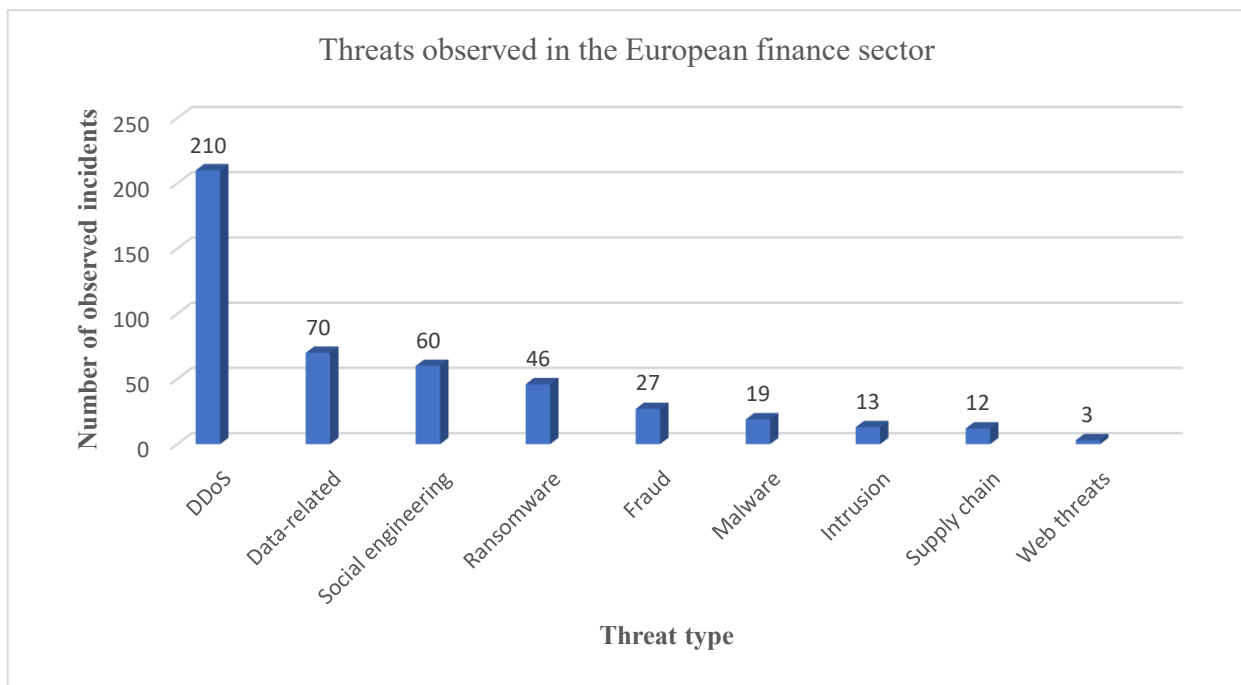
The academic literature supports a broader institutional reading of communication in cybersecurity contexts. Davis et al. (2025) show that discourse about cyber threats inside financial institutions can either create coordination or deepen division between technical and frontline personnel. This is analytically important because it suggests that communication in cyber contexts is organizationally consequential: it shapes alignment, threat interpretation, and the practical capacity of institutions to respond coherently [3].

In the EU regulatory framework, the governance relevance of such communications is embedded in positive law. DORA requires communication policies, crisis communication plans, and internal escalation arrangements for ICT-related incidents. The ECB's cyber resilience oversight expectations further require appropriate communication channels with tracking and verification of receipt for notifying management and authorities of cyber incidents [4; 5]. Taken together, these sources support the interpretation of secure communication channels as institutional coordination infrastructure rather than as a merely technical or administrative add-on.

The operational relevance of this argument is reinforced by recent sectoral threat data. ENISA's finance-sector threat landscape analyzed 488 publicly reported incidents affecting the finance sector in Europe from January 2023 to June 2024. Its threat distribution shows that DDoS attacks accounted for 210 incidents (46%), followed by data-related threats at 70 (15%), social engineering at 60 (13%), and ransomware at 46 (10%). This threat profile supports the argument that communication, escalation, and continuity are not peripheral concerns; they are central to maintaining service resilience in a sector exposed to disruptive and coordination-intensive threats [12].

This threat distribution is visualized in Figure 2, which highlights the dominance of disruptive and coordination-intensive threat categories in the European finance sector.

Figure 2 indicates that the finance-sector threat profile is dominated by disruptive and coordination-intensive categories, especially DDoS, data-related threats, social engineering, and ransomware. This strengthens the article's argument that communication, escalation, and continuity are not ancillary issues but practical conditions of resilience in the financial sector.



**Figure 2. Distribution of Observed Cyber Threats in the European Finance Sector, January 2023–June 2024**

*Note.* Prepared from ENISA finance-sector threat landscape data. The figure presents the distribution of reported threat categories affecting the European finance sector, including DDoS, data-related threats, social engineering, ransomware, fraud, malware, intrusion, supply-chain attacks, and web threats.

*Source:* Theocharidou et al. (2024) [12].

The significance of secure communication channels therefore extends beyond incident management in the narrow sense. Their role in escalation, coordination, notification, and continuity makes them directly relevant to the broader architecture of financial-sector risk governance.

### Cybersecurity, Secure Communications, and Risk Governance

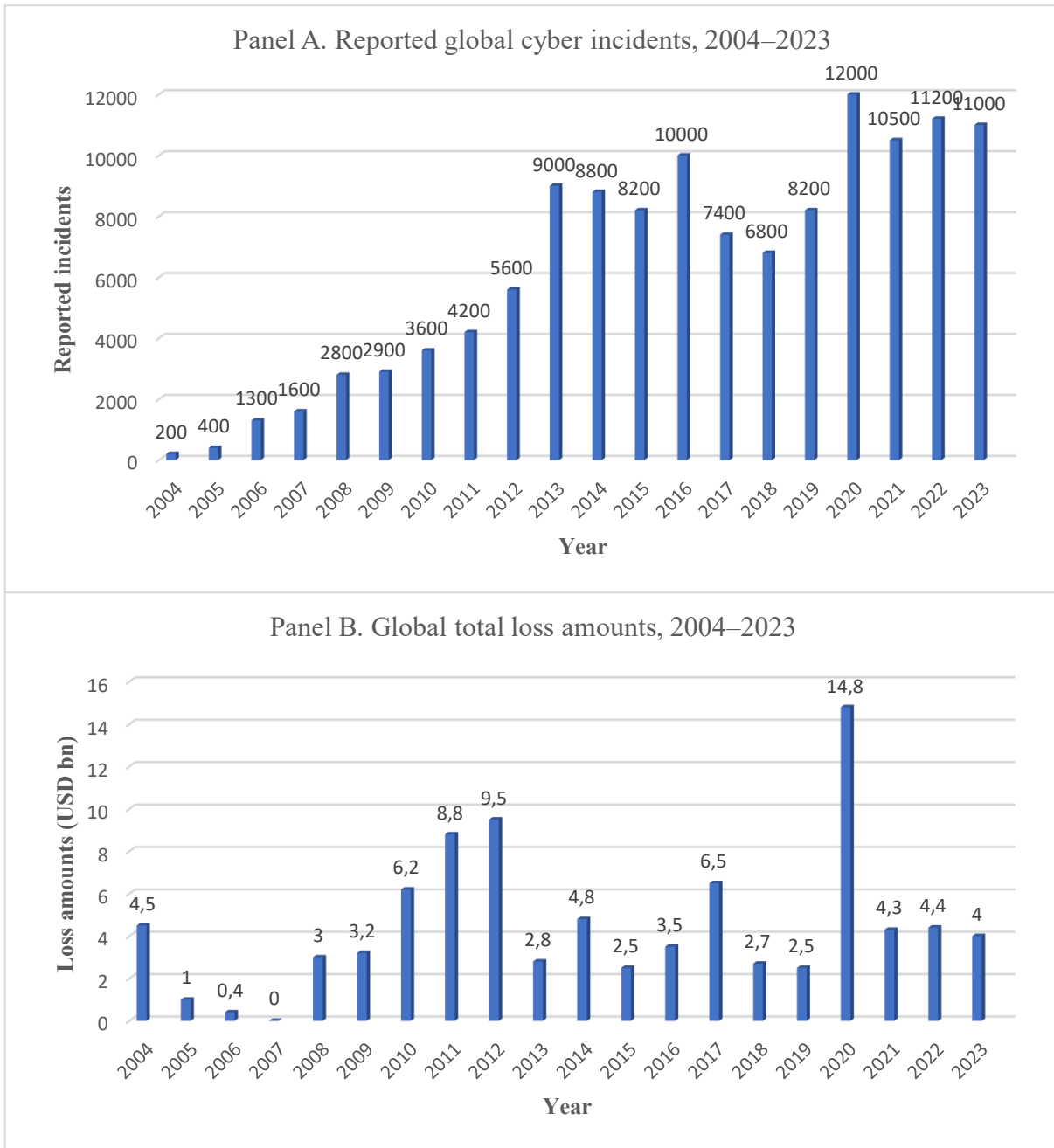
The preceding analysis suggests that cybersecurity and secure communication channels should be treated as integral elements of risk governance in the financial sector rather than as isolated operational or technical safeguards. This conclusion follows from the contemporary regulatory and resilience-oriented understanding of financial-sector risk, where ICT dependence, incident management, continuity of critical operations, and board-level accountability are increasingly managed within a unified governance architecture. DORA explicitly embeds ICT risk management, incident handling, response and recovery, communication policies, testing, and third-party risk within a single framework for digital operational resilience [5].

The connection between cybersecurity and risk governance is visible not only in regulation but also in recent scholarly work. Cojocar (2025) explicitly theorizes the alignment of regulation and governance for cyber resilience in the financial sector. When this is combined with the governance literature of Oh et al. (2025) and the financial risk-management framing of Rohmeyer and Bayuk (2019), a clearer academic picture emerges: cybersecurity in finance should be seen as part of oversight, accountability, coordination, and strategic risk architecture [2; 11; 13].

This governance interpretation is also supported by broader financial-stability evidence. The *Global Financial Stability Report* supports the view that cyber incidents have become materially relevant to financial stability discussions [8]. IMF departmental analysis further states that almost one-fifth of all reported cyber incidents in the past two decades affected the financial sector, and that total direct losses from reported cyber incidents impacting the financial sector from 2020 to 2023 stood at \$2.5 billion [7]. These figures do not capture all indirect effects, but they

reinforce the argument that cyber risk in finance is a material governance and resilience issue rather than a secondary technical concern [7; 8].

This broader financial-stability significance becomes clearer when the financial sector is viewed against the backdrop of the wider global escalation of cyber incidents and associated losses over time, as illustrated in Figure 3.



**Figure 3. Escalation of Global Cyber Risk, 2004–2023.**

*Note.* Panel A presents the time trend in reported global cyber incidents. Panel B presents the time trend in global total loss amounts associated with cyber incidents. The figure is adapted from the IMF’s published chart on selected global cyber risk metrics; the yearly values used in Panels A and B were manually approximated from the published visual and are presented here as adapted plotting data for 2004–2023.

*Source:* adapted from IMF (2024) [8] and Gaidosch et al. (2026) [7].

Figure 3 presents the broader global escalation of cyber risk along two dimensions: the rising number of reported cyber incidents and the increase in total loss amounts over time. Although these panels do not isolate the financial sector, they provide an important macro-level context for

the article's argument by showing that cyber risk has become more frequent and more costly at the global level. Against this wider trend, the material significance of cyber risk for the financial sector becomes analytically more compelling.

Table 1 provides a compact comparative synthesis of the main governance dimensions discussed in this section.

**Table 1. Comparative Governance Matrix: Cybersecurity and Secure Communication Channels in the Architecture of Digital Transformation Risk Governance**

Dimension	Digital transformation risk	Cybersecurity role	Secure communication role	Governance implication	Source
ICT dependence	Higher operational exposure and ICT concentration	Protection and resilience of critical functions	Reliable flow of trusted information during disruption	ICT risk becomes a governance matter	European Parliament & Council of the European Union (2022)
Incident response	Cross-functional escalation and restoration needs	Detection, response, recovery	Escalation, coordination, notification	Governance must remain functional under disruption	Financial Stability Board (2020)
Business continuity	Dependence on continuous digital services	Continuity of critical operations	Crisis coordination and recovery support	Continuity planning must include communications	Basel Committee on Banking Supervision (2021); ECB (2018)
Reporting and escalation	Faster supervisory and internal accountability demands	Incident classification and management	Internal and external escalation and notification	Accountability depends on communication discipline	European Parliament & Council of the European Union (2022); ECB (2018)
Third-party risk	Dependencies on suppliers and external infrastructures	Oversight of third parties	Coordination across disrupted ecosystems	Governance extends beyond internal systems	European Parliament & Council of the European Union (2022); WEF (2026)
Supervisory interaction	More formal resilience expectations	Cyber-risk governance auditability	Verifiable and communication with authorities	Supervisory traceability becomes part of resilience	Gaidosch et al. (2026); ECB (2018)

**Source:** author-compiled from Basel Committee on Banking Supervision (2021) [1], ECB (2018) [4], European Parliament & Council of the European Union (2022) [5], Financial Stability Board (2020) [6], Gaidosch et al. (2026) [7], and World Economic Forum (2026) [14].

As summarized in Table 1, the article's core argument is not that cybersecurity and communication are two separate policy concerns, but that they operate together within the governance architecture of digital transformation risk in finance. Cybersecurity provides the control and resilience logic, while secure communication channels make that logic operationally effective during escalation, disruption, and recovery.

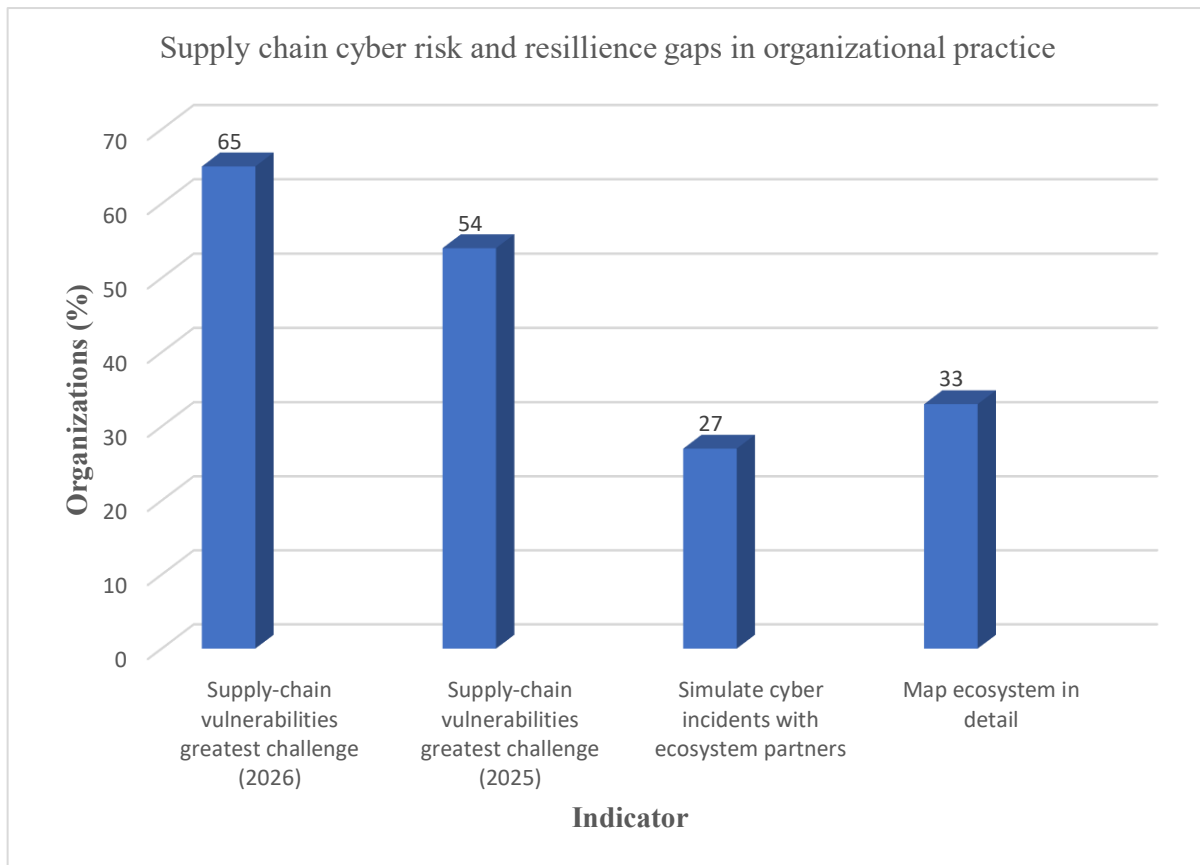
### Regulatory and Managerial Implications for the Financial Sector

If cybersecurity and secure communication channels are treated as strategic enablers of digital transformation and integral components of risk governance, then they cannot remain confined to technical departments or be addressed only through fragmented compliance measures. Contemporary regulatory frameworks increasingly require financial entities to embed ICT risk,

incident response, communication, testing, and third-party dependencies into a structured resilience architecture. In practice, this means that cybersecurity must be elevated to the level of board and senior management oversight.

A second implication concerns the institutional status of secure communication channels. Because DORA requires communication policies, crisis communication plans, internal escalation procedures, and reporting arrangements for major ICT-related incidents, financial institutions should treat secure communications as part of their control environment: they must be planned, assigned, tested, and integrated into incident governance rather than improvised during disruption.

Supply-chain and ecosystem evidence reinforces this conclusion. WEF’s *Global Cybersecurity Outlook 2026* reports that 65% of large companies by revenue identified third-party and supply chain vulnerabilities as their greatest challenge to becoming cyber resilient, up from 54% in 2025. It also reports that in financial services, the top supply-chain cyber risk is visibility — lack of visibility into the extended supply chain — while the second is concentration risk, meaning excessive dependence on critical third-party suppliers. Yet only 27% of organizations simulate cyber incidents or conduct recovery exercises with ecosystem partners, and only 33% comprehensively map their supply-chain ecosystems to understand exposure and interdependencies [14]. These findings strongly support the argument that secure communications and coordination are part of resilience governance, especially where dependencies extend beyond the firm itself. These ecosystem-level vulnerabilities and preparedness gaps are summarized in Figure 4, which provides a compact visual representation of the organizational weaknesses most relevant to resilience governance.



**Figure 4. Supply-Chain Cyber Risk and Resilience Gaps in Organizational Practice**

*Note.* Author-compiled based on World Economic Forum data. The figure shows reported supply-chain cyber resilience gaps in organizational practice, including third-party vulnerability concerns, ecosystem exercise practices, and ecosystem mapping efforts.

*Source:* World Economic Forum (2026) [14].

Figure 4 highlights that resilience gaps persist not only at the level of internal controls but also across organizational ecosystems. Because finance is deeply embedded in third-party and supply-chain relationships, these findings support the argument that communication and coordination arrangements must be understood as part of resilience governance extending beyond the boundaries of individual firms.

Table 2 summarizes how communication is positioned across the resilience-oriented frameworks reviewed in this article.

**Table 2. Communication as a Governance Mechanism in Cyber Resilience, Incident Response, and Operational Continuity Frameworks**

Source	What is said about communication	Governance meaning	Relevance for financial institutions
Financial Stability Board (2020)	Coordination and communication are core components of cyber incident response and recovery	Communication is part of organized incident response capability	Incident governance fails without trusted coordination
ECB (2018)	Communication channels should support notification with tracking and verification of receipt	Communication is tied to accountability and escalation discipline	Verifiable notification and matters for management and authorities
European Parliament & Council of the European Union (2022)	DORA requires communication policies, crisis and escalation/reporting arrangements	Communication is embedded in ICT governance	Secure communications risk are part of compliance and resilience
Gaidosch et al. (2026)	Incident-reporting supervisory coordination, exercises are part of good practice	Communication is part of and sectoral preparedness and oversight	Institutions must communicate reliably beyond firm boundaries

*Source: author-compiled from Financial Stability Board (2020) [6], ECB (2018) [4], European Parliament & Council of the European Union (2022) [5], and Gaidosch et al. (2026) [7].*

Table 2 clarifies that communication is not treated in the reviewed frameworks as a peripheral disclosure activity. It appears instead as a governance mechanism that links response capability, accountability, escalation, and preparedness across institutional and supervisory levels.

## Discussion

The analysis developed in this article suggests that cybersecurity and secure communication channels should be interpreted more broadly than is often the case in narrowly technical or compliance-driven discussions. The main significance of the findings is that they reposition these elements within the governance architecture of digitally transformed financial institutions. Rather than functioning only as protective or administrative mechanisms, they appear as enabling conditions for resilience, continuity, accountability, escalation, and coordinated response under conditions of disruption.

This matters for financial-sector cybersecurity governance because the digital transformation of finance does not merely increase technological dependence; it also changes the institutional conditions under which risk must be governed. As ICT infrastructures, third-party dependencies, and real-time operational interconnections expand, the ability of an institution to govern disruption increasingly depends on whether cybersecurity capabilities and trusted communication arrangements are embedded in governance structures rather than isolated in technical units. In this sense, the article's findings support a shift from viewing cybersecurity as a supporting IT function to viewing it as governance-relevant infrastructure.

The practical interpretive value of this argument lies in its implications for institutional design. If cybersecurity is treated as an element of governance, then board oversight, senior management accountability, resilience planning, incident escalation, and communication procedures must be aligned accordingly. Secure communication channels are especially important in this context because they help preserve the integrity of coordination when routine channels are

degraded, contested, or unavailable. Their role is therefore not limited to message transmission. They support trusted escalation, decision continuity, coordination across internal and external actors, and auditable interaction with supervisory authorities and counterparties.

This governance-oriented interpretation is particularly relevant in the financial sector, where disruptions can propagate quickly across interconnected systems and where institutional trust is closely linked to continuity, transparency, and timely response. Seen in this light, secure communication channels should not be treated as secondary administrative tools appended to incident management. They should be understood as part of the operational infrastructure through which governance remains functional during crisis conditions. The broader implication is that resilience in digitally transformed finance depends not only on defensive controls, but also on the institutional capacity to communicate securely, escalate reliably, and coordinate credibly under pressure.

### **Limitations**

This study has several limitations that should be stated explicitly. First, it is not an empirical case study and does not rely on original fieldwork, interviews, experiments, or institution-level quantitative testing. Its design is conceptual, regulatory-analytical, and synthetic, which means that the argument is developed through interpretation and integration of existing frameworks, literature, and selected analytical evidence rather than through direct observation of organizational practice.

Second, the figures included in the article rely on secondary analytical datasets and institutional evidence rather than on original author-generated datasets. These exhibits are used to strengthen the article's analytical proof layer and to illustrate the material relevance of cyber risk in the financial sector, but they do not transform the study into a primary empirical investigation.

Third, the article does not directly measure the causal effect of secure communication arrangements on resilience outcomes, incident-response performance, or governance quality. While the reviewed frameworks and literature support the interpretation that secure communications are governance-relevant and operationally significant, the present study does not test that relationship through causal research design.

Fourth, the conclusions should therefore be interpreted as a governance framework and an analytically substantiated conceptual model rather than as a universally validated causal explanation. The article is intended to clarify institutional logic, integrate fragmented literatures, and support a stronger governance interpretation of cybersecurity and secure communication channels in finance. Future research may build on this contribution through case studies, comparative institutional analysis, survey-based research, or other empirical designs capable of testing the relationships discussed here more directly.

### **CONCLUSIONS**

This article has argued that cybersecurity and secure communication channels should be understood as strategic enablers of digital transformation and as integral elements of risk governance in the financial sector. In an environment shaped by ICT dependence, operational interconnection, third-party concentration, and heightened resilience expectations, cybersecurity can no longer be treated adequately as a peripheral technical safeguard. It functions as part of the institutional architecture through which financial entities maintain continuity, comply with regulatory requirements, coordinate response, and preserve stakeholder trust under disruptive conditions.

The analysis has also shown that secure communication channels are not merely supportive administrative tools. Their role in escalation, verification, crisis coordination, supervisory interaction, and recovery makes them governance-relevant infrastructure within digitally transformed finance. When ordinary communication environments are impaired or unreliable, the institutional capacity to communicate securely becomes part of the capacity to govern effectively.

The contribution of the article is therefore primarily conceptual and integrative. By connecting regulatory frameworks, resilience-oriented supervisory logic, selected scholarly literature, and sectoral analytical evidence, it supports a governance interpretation in which cybersecurity and secure communications are structurally embedded within financial-sector resilience. On this basis, the article concludes that digitally transformed finance requires not only stronger technical protection, but also stronger governance architectures capable of sustaining trusted coordination, accountable decision-making, and resilient institutional response.

---

### Article Declarations

**Funding:** Not applicable.

**Author Contributions:** Conceptualization: P.F., S.Z.; Methodology: P.F., S.Z.; Formal analysis: S.Z.; Writing—original draft: P.F.; Writing—review & editing: P.F., S.Z. All authors have read and agreed to the published version of the manuscript.

**Conflicts of Interest:** The authors declare no conflicts of interest.

**Acknowledgements:** Not applicable.

**Data Availability:** No new primary empirical data were created for this study. The article is based on publicly available secondary sources and analytical materials cited in the References. Data sharing is therefore not applicable.

**AI Use Disclosure:** During the preparation of this manuscript, the authors used ChatGPT (OpenAI) solely for language editing, grammar correction, and improving the readability of the text. The authors remain fully responsible for the accuracy, originality, and integrity of the manuscript and confirm that no generative AI was used to fabricate data, generate scientific results, or produce misleading interpretations.

**Corresponding Author:** Pawel Frankiewicz (email: pawelfrankiewicz@gmail.com)

### REFERENCES

1. Basel Committee on Banking Supervision. (2021). *Principles for operational resilience*. Bank for International Settlements. Available at: <https://www.bis.org/bcbs/publ/d516.htm>
2. Cojocaru, A. (2025). Aligning regulation and governance for cyber resilience: A theoretical framework for the UK financial sector. *Computers & Security*, 157, Article 104627. <https://doi.org/10.1016/j.cose.2025.104627>
3. Davis, J., Maddini, S., Kankala, S., Ravindran, R. K., Kunkulagunta, M., Maturi, M. H., Nadella, G. S., & De La Cruz, E. (2025). Decoding cybersecurity discourse and communication dynamics in financial institutions. *Journal of Responsible Technology*, 24, Article 100142. <https://doi.org/10.1016/j.jrt.2025.100142>
4. European Central Bank. (2018). *Cyber resilience oversight expectations for financial market infrastructures*. European Central Bank. Available at: [https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber\\_resilience\\_oversight\\_expectations\\_for\\_financial\\_market\\_infrastructures.pdf](https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf)
5. European Parliament & Council of the European Union. (2022). *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. *Official Journal of the European Union*, L 333, 1–79. Available at: <http://data.europa.eu/eli/reg/2022/2554/oj>

6. Financial Stability Board. (2020). *Effective practices for cyber incident response and recovery: final report*. Financial Stability Board. <https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery-final-report>
7. Gaidosch, T., Islam, E., Khiaonarong, T., Ravikumar, R., & Walker, C. (2026). *Good practices in cyber risk regulation and supervision* (Departmental Paper No. 2026/001). International Monetary Fund. <https://doi.org/10.5089/9798229026185.087>
8. International Monetary Fund. (2024). *Global financial stability report: The last mile—Financial vulnerabilities and risks*. Available at: <https://www.imf.org/en/publications/gfsr/issues/2024/04/16/global-financial-stability-report-april-2024>.
9. Khiaonarong, T., & Zheng, S. (2026). *The rise of cyber events and digital fraud in the financial sector* (IMF Working Paper No. 2026/062). International Monetary Fund. <https://doi.org/10.5089/9798229043557.001>
10. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper 29). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>
11. Oh, K. B., Hoang, G., Sturdy, J., & Guo, S. S. (2025). *Cybersecurity governance: An enterprise risk management strategy for cyber risk control*. Springer. <https://doi.org/10.1007/978-981-95-3865-2>
12. Theocharidou, M., Lella, I., Naydenov, R., & Malatras, A. (2024). *ENISA threat landscape: Finance sector, January 2023 to June 2024*. European Union Agency for Cybersecurity. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector>
13. Rohmeyer, P., & Bayuk, J. L. (2019). *Financial cybersecurity risk management: Leadership perspectives and guidance for systems and institutions*. Apress. <http://doi.org/10.1007/978-1-4842-4194-3>
14. World Economic Forum. (2026). *Global cybersecurity outlook 2026*. World Economic Forum. Available at: <https://www.weforum.org/publications/global-cybersecurity-outlook-2026/>

---

**Article History:**

Received: February 23, 2026 | Revised: March 20, 2026 | Accepted: April 06, 2026 | Published Online: April 15, 2026

**Citation:** Frankiewicz, P., & Zahranychnyi, S. (2026). CYBERSECURITY AND SECURE COMMUNICATION CHANNELS AS STRATEGIC ENABLERS OF DIGITAL TRANSFORMATION AND RISK GOVERNANCE IN THE FINANCIAL SECTOR. *International Interdisciplinary Scientific Journal "Expert"*, 3, Article 2, 1–13. <https://doi.org/10.62034/2815-5300/2026-v3-002>



Provides free access under the Gold Open Access model with costs covered by APCs.

This article is permanently accessible online and can be freely used, shared, or adapted, provided proper attribution is given.



This work is licensed under the Creative Commons Attribution 4.0 International (CC BY 4.0).