DETERMINING THE OPTIMAL INVESTMENT IN SECURITY AND RECOVERY FOR PROTECTING PAYMENT SYSTEMS: A RISK-BASED APPROACH FRAMEWORK

Ela Mădălina SCARLAT[19]

Abstract: *In the modern financial landscape, the seamless provision of financial services heavily relies on technology and interconnected data systems. This digital dependency, while convenient for consumers, exposes financial institutions to heightened cyber risks from potential attackers. In light of this increased cyber threat, it has become imperative to develop an efficient cyber-risk management framework tailored to the financial sector, encompassing both institutions and their supply chain partners.*

By adopting a comprehensive risk-based approach, financial institutions and payment service providers can make data-driven decisions on the optimal investment in security and recovery for protecting payment systems. The framework enables organizations to strike a balance between risk mitigation and resource allocation, ensuring the resilience and trustworthiness of payment ecosystems in an increasingly digitized world.

This paper focuses on establishing a general framework for ensuring the cyber resilience of financial institutions, as cyber incidents can lead to severe financial and reputational impacts, potentially jeopardizing the continuity of operations for the targeted institutions. This article proposes a risk-based approach to guide decision-makers in identifying optimal investment levels in security and recovery to safeguard payment systems.

The framework proposed by this paper can be utilized by the banking sector and financial institutions to establish and implement a comprehensive cyber-resilience strategy. Emphasizing optimal safety measures, this framework aims to safeguard the financial sector's uninterrupted functionality, bolstering its ability to withstand cyber attacks effectively. By embracing a

[19] Romanian Academy, "Costin C. Kiriţescu" National Institute of Economic Research, Bucharest, Romania, email: ela.scarlat@bnro.ro

proactive and adaptive approach to cyber-risk management, financial institutions can enhance their overall resilience and better protect the interests of their customers and stakeholders.

***Keywords**: risk assessment, cyber resilience, cyber risk, financial market infrastructures, payment systems*

***JEL Classification:** O1; D5; E22; E5; E62.*

Introduction

With the rapid global digitization and the increasing reliance on technology and communication networks in the financial sector, the management of cyber risks has become an imperative concern for institutions worldwide. The accelerated pace of digitization and the ongoing evolution of cyber threats have compelled financial institutions to take proactive measures in safeguarding their operations and client data.

Some financial institutions, particularly critical banks and national payment systems, hold a central position in the financial sector, and their vulnerabilities can have far-reaching implications due to network links and the contagion effect. As a result, the cyber risk within the financial sector has the potential to generate systemic risk within the national economy under certain circumstances.

In Romania, low cyber security levels in communication infrastructures and technology gaps pose challenges for cyber resilience. The National Recovery and Resilience Plan aims to attract funds for digitalization and critical infrastructure security.

Digital transformation is a strategic goal for Romania, and cyber security is a national priority to address risks in the virtual environment. Several strategic documents underline the significance of cyber security in achieving sustainable development and national defense objectives.

As the financial system becomes increasingly technology-driven, the potential vulnerabilities associated with cyber incidents can have far-

reaching consequences, disrupting the proper functioning of financial institutions and undermining trust in the entire system. Therefore, a robust cyber risk management framework is indispensable in ensuring the resilience of financial institutions against cyber-attacks and protecting the interests of their clients and stakeholders.

In this context, this paper aims to shed light on the critical elements necessary for implementing an effective cyber risk management framework for the financial sector. By highlighting the crucial elements required for effective cyber risk management, the research seeks to provide financial institutions and regulatory bodies with valuable insights and practical guidelines to fortify their defenses against cyber threats.

The global financial landscape has witnessed a significant shift towards electronic payment systems, providing unparalleled convenience and efficiency. However, this transformation has also attracted cyber threats that continuously evolve in complexity and frequency. To protect payment systems effectively, financial institutions and payment service providers must embrace a risk-based approach that optimizes investments in security and recovery measures. A comprehensive and dedicated approach to cyber risk management will enhance the overall resilience and sustainability of the financial sector in an increasingly digitized world.

Literature review

According to BCBS Basel II, operational risk is defined as the potential for financial loss arising from deficient or unsuccessful internal processes, human resources, and systems, or due to external events. This definition encompasses legal risk while excluding strategic and reputational risks (FSB, 2023).

Operational resilience is defined as the ability of a payment system and its service providers to deliver critical operations during disasters and extreme circumstances (BIS, 2021). A financial institution's capability to recognize and shield against threats and possible failures is crucial.

Additionally, it should enable the financial institution to react, adjust, recover, and gain insights from disruptive incidents to minimize their effects on vital operations during disruptions, by anticipating disruptions and establishing their risk appetite and "tolerance for disruption" accordingly. This involves developing frameworks for risk identification, impact tolerance, interdependency mapping, and continuous testing. International principles, such as the *Principles for Financial Market Infrastructures* (PFMI), provide guidance on business continuity planning and reliability and resilience expectations for critical service providers. The tolerance for disruption, as outlined in the *Principles of Operational Resilience*, refers to the extent of operational risk disruption a financial institution is willing to withstand in the face of severe yet plausible scenarios (BIS, 2021).

Maintaining operational resilience faces challenges due to the growing demand for real-time payments, emerging technologies, increasing interdependencies and evolving risks. Coordinated and simultaneous incidents pose new challenges, necessitating cross-sectoral and cross-border crisis management arrangements involving multiple authorities and stakeholders.

Systemic cyber risk refers to the risk that a cyber event would affect critical infrastructure components, leading to significant disruptions and losses (FSB,2018). The importance of addressing this risk is recognized by the G-7 group, which emphasizes the need for cyber resilience management.

Cyber resilience involves protecting data and electronic systems from cyber attacks and quickly resuming operations after successful attacks. Both cyber security and cyber resilience strategies are essential to combat cyber threats effectively.

The evaluation methodology of cyber risks entails (ENISA, 2022): the identification of risks (categorization of assets, assessment of asset value, compilation of threat lists, compilation of vulnerability lists), the calculation of risks and addressing the risks (cataloguing of measures and the evaluation of the residual risk).

Cyber events can lead to systemic risks in the financial system through three main transmission channels: risk Concentration (attacks on critical financial infrastructures or systemically important institutions can cause irreplaceable service losses), risk contagion (cyberattacks on one financial institution can spread difficulties to others due to high interconnectedness) and erosion of confidence (widespread attacks can trigger a loss of confidence across multiple financial institutions) (Goh et. al., 2020). These risks arise from disruptions to critical financial infrastructures and interconnectedness. Confidence effects can create a self-fulfilling chain of events. Unlike traditional risks, cyber risks materialize rapidly within the financial system, demanding coordinated crisis communications and contingency plans to mitigate systemic outcomes. Policymakers must understand cyber event impacts and transmission channels to respond effectively and minimize systemic risks.

ENISA (2022) has identified and ranked the ten foremost cybersecurity threats expected to arise by 2030: compromise of software dependencies in the supply chain, sophisticated disinformation campaigns, emergence of digital surveillance authoritarianism and privacy erosion, human errors and vulnerabilities in legacy systems within cyber-physical environments, targeted attacks leveraging smart device data, inadequate analysis and control of space-based infrastructure and objects, escalation of advanced hybrid threats, shortage of skilled cybersecurity professionals, dependency on cross-border ICT service providers as a potential single point of failure and the misuse of artificial intelligence.

The comprehensive management of general business and operational risks is based on the following principles (BIS, 2012):

- proactive management of general business risk – financial market infrastructures (FMIs) must take proactive measures to identify, monitor, and manage their general business risk. To ensure uninterrupted operations in the face of potential losses, FMIs should maintain sufficient liquid net assets, funded through equity, to cover any general business losses that may occur;

- safeguarding of assets - payment systems (PS), central securities depositories (CSDs), securities settlement systems (SSS) and central counterparties (CCPs) must prioritize the protection of their own and participants' assets. Efforts should be made to minimize the risk of asset loss or delays in accessing these assets;
- mitigation of operational risk - FMIs should conduct a comprehensive assessment of all potential sources of operational risk and implement appropriate systems, policies, procedures, and controls to mitigate them. Business continuity management should be geared towards ensuring timely recovery of operations, even in the face of major disruptions.

A risk mitigation framework or approach must cover, at a minimum, the subsequent stages (ISO 27005, EU ITSRM), which can be viewed as its primary operational constituents (ENISA,2022): i) risk identification (assets, threats and vulnerabilities); ii) risk evaluation (risk computation and appraisal); iii) risk mitigation (choice and implementation of protective measures and evaluation of remaining risk); iv) risk surveillance (evaluate the efficiency of measures and supervise risks).

The interoperability between risk management frameworks can be assessed based on the following functional characteristics and levels: generic aspects (examining whether the framework adopts an asset-based or scenario-based approach and whether it uses quantitative or qualitative criteria for risk assessment); risk identification (evaluating whether the framework can use each other's asset taxonomy, valuation methods, threat, and vulnerability catalogues without negatively affecting subsequent steps); risk assessment (assessing whether the framework uses the same methodology for risk calculation or provides results that can be easily mapped to other frameworks); risk treatment (determining whether the framework results in the same set of measures or measures with an equal contribution to reducing risk levels) (ENISA, 2022). Frameworks that do not require specific methods for these functional components are considered highly interoperable, as they can accommodate risk management components from various methods.

Examples of such frameworks include NIST 800-37 and BSI Standard 200-2 (IT-Grundschutz Methodology).

In the context of digitalization and the health crisis caused by the pandemic in the years 2020-2021, which imposed physical restrictions and led to a rapid increase in online commerce, a favorable environment for financial crime was created. Authorities worldwide provided certain guidance to financial institutions during that period, particularly regarding mitigating cyber attacks and risks related to money laundering and terrorism financing. This drew attention to these offenses and increased risks, aiming to better inform financial institutions and the general public and enhance awareness among staff and customers. It underlined the importance of active information exchange between the public and private sectors at the national and international levels. The issued guidance also highlighted the need for a compromise between adjusting anti-money laundering frameworks and enhancing cyber resilience (cybersecurity incident response plans) while avoiding imposing excessive burdens that could hinder financial institutions from providing key financial services (Crisanto, Prenio, 2020).

In practice, the cybersecurity strategy of an institution involves continuous risk assessment followed by cost-benefit analysis. The cybersecurity dilemma - to pay now or pay later - entails an inherent compromise between paying to prevent a problem and paying to eliminate the effects of the problem.

Risk assessment shapes investment priorities, determining the direct and indirect risks the institution assumes, and comparing the direct costs (ransom payments or expenses associated with identifying, mitigating, and isolating a threat) and indirect costs (downtime, operational disruptions, negative impact on reputation, internal time and resources, legal and non-compliance penalties) of materializing those risks with the benefits (Shackleton, 2021).

The NIST Cyber Security Framework mentions the following components of cybersecurity assurance: identification (managing assets, processes, and key systems that need protection; considering the

business environment, supply chains, interdependencies between the institution and other institutions it interacts with and/or depends on; governance; risk assessment; risk management strategy); protection (controlled access; personnel awareness and training programs; data security; information protection procedures and processes; system maintenance; protective technology); detection (defining anomalies and suspicious events; continuous security monitoring; detection processes); response (incident response plan; communication; analysis; mitigation; improvement implementation); recovery (recovery plan; improvements; communication).

The NIST Cybersecurity Framework and the Gordon-Loeb Model suggest that organizations should generally spend less than 37% of the expected loss from a cybersecurity breach on preventive/strategic budget.

The five strategic objectives of importance in Romania for the period 2022-2027 in the field of cybersecurity are: secure and resilient networks and information systems; consolidated regulatory and institutional framework; pragmatic public-private partnership; resilience through proactive approach and deterrence; international collaboration. The specific measures to achieve these objectives are included in the Action Plan for the implementation of Romania's Cybersecurity Strategy for the period 2022-2027 and represent a shared responsibility of all actors involved.

Methodology

The qualitative research methodology employed in this study involves a comprehensive review and analysis of relevant specialized literature and legislation pertaining to cyber resilience in credit institutions and payment systems. The research methodology integrates practical studies, theoretical analysis and logical discourse to establish the understanding of cyber risk assessment and mitigation, in the context of the digital economy.

The data for this research was collected through a systematic search of scholarly articles, research papers, industry reports, regulatory documents, and relevant legislative frameworks related to cyber resilience in credit institutions and payment systems. Online databases, academic journals, and authoritative sources in the field of cybersecurity and risk management were consulted to ensure the inclusion of the most recent and reliable information. The collected data was subjected to rigorous qualitative analysis techniques, including thematic analysis and content analysis. The goal was to identify recurring themes, patterns, and insights related to risk assessment, vulnerability identification, risk mitigation, operational resilience, interdependency risks, and the integration of security and recovery measures in payment systems.

Based on the analysis of the literature and legislation, a general and structured framework that guides a financial institution in evaluating and mitigating cyber risk was developed. This framework aims to address the challenges faced by financial institutions and payment service providers in safeguarding payment systems against evolving cyber threats and operational disruptions. It advocates a risk-based approach that takes into account the identified vulnerabilities, threats, and potential impacts on payment systems, allowing for the optimal allocation of resources for security measures and recovery capabilities.

The qualitative approach was chosen due to its ability to provide a deep understanding of complex phenomena, allowing exploration and gaining insights into the challenges and best practices associated with cyber-risk management and payment system security. Qualitative research allows for a nuanced examination of various risk factors, vulnerabilities, and potential impacts on payment systems, enabling a more holistic perspective on cyber-resilience.

Further research is required to develop decision-making models that can determine the ideal level of investment in risk reduction, resilience and recovery strategies for cyber disasters, but such models need to consider the specific vulnerabilities of each entity, making generalized approaches to optimal investment unfeasible. Additionally, there is a need for user-

friendly cyber risk analysis models that can identify vulnerabilities at both the entity and financial sector levels.

Another factor that the framework did not address is incentivizing participants and customers to contain the risks they pose, where applicable.

Results and discussions

Credit institutions play a central role in the payment market as the primary providers of financial services to consumers. It is essential for these institutions to ensure efficient and secure operations while delivering their services. Currently, critical participants in the payment systems are some of the credit institutions.

A comprehensive risk assessment framework is fundamental to identify potential threats, vulnerabilities, and impacts on payment systems. By analyzing historical attack patterns, assessing emerging risks, and understanding industry-specific vulnerabilities, organizations can prioritize security and recovery investments effectively.

The framework proposed below aims to address the challenges faced by financial institutions and payment service providers in safeguarding payment systems against evolving cyber threats and operational disruptions. It advocates a risk-based approach to determine the optimal allocation of resources for security measures and recovery capabilities while considering residual risk. The framework emphasizes the importance of continuous monitoring, regular risk assessments, and adaptation to maintain the effectiveness of security and recovery strategies.

Identifying and Managing Risks

Comprehensive analysis of the current threat landscape is crucial to identify potential cyber threats and attack vectors targeting payment systems. Examining past cyber incidents, assessing emerging threats, and understanding cyber adversaries' tactics, techniques, and procedures (TTPs) are essential components of this analysis.

Operational risks, whether internal or external, can significantly impact the functioning of a PPS. Adequate systems, policies, procedures, and controls must be put in place to mitigate their impact. Ensuring a high degree of security, operational reliability and scalable capacity is crucial. Business-continuity management should be designed to ensure timely recovery of operations and fulfillment of obligations during disruptions.

Interdependency Risks: PPS should regularly review risks arising from interdependencies with other entities and develop risk management tools to address them. Additionally, risks posed by key participants, other Financial Market Infrastructures (FMIs), payment service providers, and utility providers should be identified, monitored, and managed.

The financial institution must establish risk management policies, procedures, and systems to identify, measure, monitor, and manage various risks faced by the payment system. This involves examining historical attack patterns, emerging threats, and industry-specific risks.

Identifying Vulnerabilities and Potential Impact

Conducting vulnerability assessments and penetration testing helps payment service providers identify weaknesses in their systems. Mapping these vulnerabilities against potential financial losses and reputational damage provides insights into cyberattack risks.

Risk Assessment

Quantifying the probability and impact of various cyber threats through a risk assessment process allows institutions to evaluate inherent risk.

The risk assessment shapes investment priorities by identifying the direct and indirect risks that an institution assumes. It involves comparing the direct costs (ransom payments or expenses associated with identifying, mitigating, and isolating a threat) and the indirect costs (downtime, operational disruptions, negative impact on reputation, internal time and resources, legal and regulatory sanctions) of materializing those risks with the benefits (Shackleton, 2021).

A risk mitigation framework should cover stages like risk identification, evaluation, treatment, and surveillance. Highly interoperable frameworks can accommodate risk management components from various methods.

Systemic Cyber Risk

Systemic cyber risk refers to the risk that a cyber event would affect critical infrastructure components, leading to significant disruptions and losses. Organizations must understand cyber event impacts and transmission channels to respond effectively and minimize systemic risks.

Operational Resilience

Operational resilience is the ability of a payment system and its service providers to deliver critical operations during disasters and extreme circumstances. Organizations should establish frameworks for risk identification, impact tolerance, interdependency mapping, and continuous testing. This includes maintaining sufficient liquid net assets funded through equity to cover any general business losses that may occur.

Cost-Benefit Analysis

Conducting a cost-benefit analysis is vital to determine the economic impact of potential security and recovery investments. This analysis compares the costs of implementing preventive measures and recovery capabilities with the potential benefits of mitigating risks and preventing financial losses. It ensures resource allocation aligns with risk mitigation efforts.

Operational Risk Mitigation

For operational risks, both internal and external, Payment and Settlement Systems (PPS) should identify plausible sources and mitigate their impact using suitable systems, policies, procedures, and controls. These systems should prioritize high security and operational reliability and possess adequate, scalable capacity. Business continuity management should

ensure timely recovery of operations and fulfillment of obligations, even in the face of wide-scale or major disruptions.

Key considerations involve establishing a robust operational risk management framework, clearly defining roles and responsibilities at the board level, and subjecting systems, policies, procedures, and controls to regular review, audits, and testing. Operational reliability objectives should be well-defined and supported by policies.

A risk mitigation framework should cover stages like risk identification, evaluation, treatment, and surveillance. Highly interoperable frameworks can accommodate risk management components from various methods.

The PPS must ensure scalable capacity to handle increasing stress volumes and achieve service-level objectives. PPS should ensure scalable capacity to handle increasing stress volumes and comprehensive physical and information security policies to address potential vulnerabilities and threats. Regular reviews, audits, and testing should validate the effectiveness of security measures.

Comprehensive physical and information security policies should address potential vulnerabilities and threats.

A robust business continuity plan, incorporating a secondary site, should be in place to mitigate disruption impact and facilitate settlement by the end of the disruption day, even under extreme circumstances. Regular testing of these arrangements is crucial.

Additionally, risks posed by key participants, other FMIs, payment service providers, and utility providers should be identified, monitored, and managed.

A well-defined *business continuity plan* should be in place to address disruptions, incorporating the use of a secondary site and enabling the PPS to complete settlement by the end of the disruption day, even under extreme circumstances. Regular testing of these arrangements is essential to verify their effectiveness.

Aligning Investments with Risk Mitigation: Based on risk assessment results and cost-benefit analysis, organizations can prioritize investments that address critical vulnerabilities and provide the highest risk reduction.

This ensures resources are optimally allocated to protect payment systems.

Recovery Plans

A PPS is expected to identify scenarios that could prevent it from providing critical operations and services as a going concern and assess the effectiveness of recovery or orderly wind-down options. Based on this assessment, the PPS should prepare appropriate plans for recovery or orderly wind-down and provide relevant authorities with information for resolution planning, if applicable. The PPS should maintain a viable recovery or orderly wind-down plan and hold sufficient liquid net assets to implement it, in addition to resources for covering participant defaults or other risks covered under credit and liquidity risk management standards.

Accordingly, appropriate recovery plans should be developed based on these assessments, and relevant authorities should be provided with the necessary information for resolution planning when applicable.

Integration of security and recovery

Effective protection of payment systems requires an integrated approach, combining proactive security measures with robust recovery strategies.

Based on risk assessments and cost-benefit analysis, institutions can prioritize security and recovery measures. High-risk areas warrant more significant investment to enhance defenses and recovery capabilities, while areas with high potential impact but relatively low inherent risk may benefit from recovery-focused strategies.

It is notable that low probability-high impact threats need to be treated adequately, no matter the risk tolerance accepted.

Strengthening Security Investment:

Investments in security measures should focus on mitigating known and emerging cyber threats. Implementing technologies such as firewalls,

intrusion detection systems, encryption, and multi-factor authentication can bolster the security posture. Continuous monitoring and employee training are vital components of a proactive security approach.

Enhancing Recovery Investment:

Recovery capabilities are equally important in safeguarding payment systems. Organizations must develop comprehensive incident response plans, implement redundancy and data backups, and regularly conduct recovery exercises to validate effectiveness.

Residual Risk Evaluation

The residual risk, on the other hand, considers the effectiveness of existing security measures in mitigating risks, as mitigation measures can reduce the risk, but they can not eliminate it.

Calculating the residual risk, which remains after implementing security and recovery measures, is crucial in determining the effectiveness of existing controls. By quantifying the level of risk exposure, organizations can make informed decisions on additional risk mitigation measures.

Considering cyber-insurance

Combining security investments and cyber-insurance represents a synergistic approach to cyber-risk management, allowing for the optimization of the overall security expenses, as an alternative approach to risk management involves transferring the risk to a third party, typically achieved through insurance. In this context, the insurer assumes the risk in exchange for periodic premium payments by the insured. The *residual risk* could be covered by cyber-insurance.

While much of the literature has focused on the insurability and growth of the cyber-insurance market, recent research indicates that the market is set to expand with institutional support.

Efforts have been made to develop pricing formulas for insurance premiums using established risk models, allowing for a more operational approach to cyber-insurance. However, it's important to note that

security investments and cyber-insurance are not mutually exclusive options. They can work synergistically to address cyber-risks, employing a mix of strategies. By investing in security measures, vulnerabilities can be reduced, leading to lower insurance premiums. Consequently, security investments and insurance can be jointly optimized to minimize overall security expenses.

When considering the presence of correlation between security incidents, the optimal risk management mix needs to be reevaluated.

For multi-branch companies, security breaches in any branch may have repercussions on the security of the headquarters. Therefore, risk management decisions must be reconsidered, accounting for vulnerability correlation. Despite its significance, the impact of vulnerability correlation on risk management strategy optimization has not been extensively explored in the literature.

The investigation of optimal strategies for a multi-branch company, involving both insurance and security investments to mitigate security-related losses, sheds light on the impact of vulnerabilities in the branches on the headquarters' behavior. Surprisingly, as the vulnerability of branches increases, the headquarters tend to invest less in security and rely more on insurance, suggesting a counterintuitive relationship. This phenomenon is particularly pronounced when branch vulnerability is either very low or very high, as it becomes less beneficial to invest in security measures. Notably, no investment is recommended in regions of very low or very high vulnerability (Mazzoccoli, Naldi, 2021).

Continuous Monitoring and Review

A risk-based approach requires continuous monitoring and evaluation to stay abreast of evolving threats and ensure the effectiveness of security and recovery measures. Regular adjustments and adaptations are essential to maintain the resilience of payment systems. Investing in security and recovery is an ongoing process. Continuous monitoring of the threat landscape, regular risk assessments, and periodic reviews of security measures are crucial for maintaining an optimal investment strategy.

The framework can be supplemented with case studies that highlight real-world examples of organizations that have successfully implemented risk-based approaches to optimize investment in security and recovery for their payment systems. These case studies provide valuable insights into best practices and lessons learned.

Conclusion

A proactive and risk-based approach is essential to protect financial institutions effectively. By understanding the evolving threat landscape, identifying vulnerabilities, conducting risk assessments and integrating security and recovery measures, financial institutions can make informed decisions on optimal investment. A well-balanced investment strategy ensures effective risk management, stability, and trustworthiness of digital payment ecosystems. Furthermore, incorporating additional measures such as impact tolerance setting, business continuity arrangements, tandem processing, and resilient information security will further strengthen the operational resilience of payment systems, bolstering security and efficiency against various challenges and disasters effectively.

The effective management of risks in Payment and Settlement Systems and the risks of their critical participants is crucial for the stability and integrity of financial markets. The continuous evolution of payment systems requires ongoing efforts to strengthen operational resilience. Understanding and managing operational risks, enhancing interdependency management, and developing comprehensive business continuity plans are essential for ensuring the efficient functioning of payment systems under adverse conditions. By addressing these challenges and drawing lessons from past incidents, payment systems can enhance their resilience and contribute to a more stable financial environment.

The framework emphasizes the identification, measurement, monitoring and management. Furthermore, it outlines the need for a well-defined

operational risk management system, business continuity planning, and recovery plans to ensure a financial institution's ability to recover or wind-down operations effectively in adverse scenarios.

Cyber risk management practices should not solely rely on reactive controls but also encompass proactive protection against future cyber events. The ability to predict and anticipate such events relies on analyzing deviations from established benchmarks that define normal behavioral activity within the system.

The threat landscape and the payments ecosystem are dynamic and ever-changing. Organizations must adopt a proactive stance by continually monitoring and reassessing risks, updating security measures, and adapting recovery strategies to stay ahead of emerging threats. Continuous improvement and adaptation are key elements in mitigating potential disruptions. Regular review and periodic updates of risk management frameworks are essential.

References

Bank for International Settlements (2012). Principles for financial market infrastructures, April, https://www.bis.org/cpmi/publ/d101.htm

Bank for International Settlements (2012). Assessment methodology for the principles for FMIs and the responsibilities of authorities. Consultative report, April, https://www.bis.org/cpmi/publ/d101b.pdf

Bank for International Settlements (2012). Principles for financial market infrastructures: Disclosure framework and Assessment methodology, December, available at: https://www.bis.org/cpmi/publ/d106.pdf

Bank for International Settlements (2001). Core Principles for Systematically Important Payment Systems, January, https://www.bis.org/cpmi/publ/d43.pdf

Bank for International Settlements (2021). Principles for Operational Resilience, Basel Committee on Banking Supervision, March, https://www.bis.org/bcbs/publ/d516.pdf

Bank for International Settlements (2016). Guidance on cyber resilience for financial market infrastructures, June, https://www.bis.org/cpmi/publ/d146.pdf

Bank of Canada (2016). Criteria and Risk-Management Standards for Prominent Payment Systems, https://www.bankofcanada.ca/wp-content/uploads/2016/02/criteria-risk-management-standards.pdf

Boyens, J.; Smith, A.; Bartol, N.; Winkler, K.; Holbrook, A.; Fallon, M. (2022). Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST Special Publication NIST SP 800-161r1, May, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

Center for Strategic and International Studies (CSIS). Significant Cyber Incidents, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Chioncel, M. (2021), Analysis of the factors that obstruct the diffusion of innovation, Increasing the capacity of the RDI system to respond to global challenges. Strengthening anticipatory capacity to develop evidence-based public policies", POCA 127557, SIPOCA 592, December, https://www.poc.research.gov.ro/uploads/2021-2027/conditie-favorizanta/analysis-of-the-factors-that-obstruct-the-diffusion-of-innovatio.pdf

Dragoman, S., Chiriță, G., Chiffa, M., Pârâială, A., Tutunaru, C. & Pădureanu, V. (2021). Barierele Digitalizării mediului public şi privat din România, Autoritatea pentru Digitalizarea României, April, https://www.poc.research.gov.ro/uploads/2021-2027/conditie-favorizanta/bariere-digitalizare.pdf

European Central Bank. Cyber resilience and financial market infrastructures, https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html

European Central Bank. What is cyber resilience?, https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html

European Commission (2020). The EU's Cybersecurity Strategy for the Digital Decade, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Commission (2021). Romania in the Digital Economy and Society Index, https://digital-strategy.ec.europa.eu/en/policies/desi-romania

European Commission (2014). The European Cyber Defence Policy, https://www.european-cyber-defence-policy.com/

European Council (2022). The NIS 2 Directive, https://www.nis-2-directive.com/

European Council (2022). The Digital Operational Resilience Act (DORA), https://www.digital-operational-resilience-act.com/

European Council (2017). Cyber attacks: EU ready to respond with a range of measures, including sanctions, https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

European Systemic Risk Board (2020). Systemic cyber risk, European System of Financial Supervision, February, ISBN 978-92-9472-131-0, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

European Union Agency for Cybersecurity (2020). ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected, https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

FATF, Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Rba-npps-2013.html

FATF (2014), The banking sector. Guidance for a risk-based approach, October, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Banking-Sector.pdf.coredownload.pdf

Financial Stability Board (2023). Cyber Lexicon, https://www.fsb.org/wp-content/uploads/P130423-3.pdf

Financial Stability Board (2018). Cyber Lexicon https://www.fsb.org/2018/11/cyber-lexicon/

G-7 (2016). G7 Fundamental elements of cybersecurity for the financial sector, October, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

G-7 (2017). G-7 Fundamental elements for effective assessment of cybersecurity in the financial sector, https://www.ecb.europa.eu/paym/pol/shared/pdf/October_2017-G7-fundamental-elements-for-effective-assessment-of-cybersecurity-in-the-financial-sector.en.pdf

G7 (2018). G7 Principles and Actions on Cyber, https://ccdcoe.org/uploads/2018/11/G7-160527-G7PrinciplesAndActions-1.pdf

G-7 (2022). G7 Fundamental elements for third party cyber risk management in the financial sector, October, https://www.ecb.europa.eu/paym/pol/shared/pdf/ October_2022-G7-fundamental-elements-for-third-party-cyber-risk-management-in-the-financial-sector.en.pdf

G7 (2018). G7 Fundamental Elements for Threat-Led Penetration testing, https://www.ecb.europa.eu/paym/pol/shared/pdf/October_2018-G7-fundamental-elements-for-threat-led-penetration-testing.en.pdf

G7 (2020). G-7 Fundamental elements of cyber exercise programmes, https://www.gov.uk/government/publications/g-7-fundamental-elements-of-cyber-exercise-programmes/g-7-fundamental-elements-of-cyber-exercise-programmes

G-7 (2022). G7 Fundamental elements of ransomware resilience for the financial sector, October, https://www.ecb.europa.eu/paym/pol/shared/pdf/October_2022-G7-Fundamental-elements-of-ransomware-resilience-for-the-financial-sector.en.pdf

Kaffenberger, L. & Kopp, E. (2019). Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment, Carnegie Endowment for

International Peace Publications Department, https://carnegie-endowment.org/2019/09/30/cyber-risk-scenarios-financial-system-and-systemic-risk-assessment-pub-79911

Kaffenberger, L., Kopp, E. & Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability, International Monetary Fund, August, https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104

Kantar Public (2022). Study on New Digital Payment Methods, March, available at: https://www.ecb.europa.eu/paym/digital_euro/ investigation/profuse/shared/files/dedocs/ecb.dedocs220330_report.en.pdf

Khiaonarong, T.; Leinonen, H.; Rizaldy, R. (2021), Operational Resilience in Digital Payments: Experiences and Issues, https://www.elibrary.imf.org/view/journals/ 001/2021/288/article-A001-en.xml

Mazzoccoli, A.; Naldi, M. (2021). Optimal Investment in Cyber-Security under Cyber Insurance for a Multi-Branch, Firmhttps://ideas.repec.org/a/gam/jrisks/v9y2021i1p24-d479033.html

McGuire, M. (2018). Into the web of profit. Understanding the growth of the cybercrime economy, Bromium Inc., April, https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf

Ministry of Research, Innovation and Digitalization (2022). Romania's National Strategy for Research, Innovation and Smart Specialization 2022-2027, July, https://www.poc.research.gov.ro/uploads/2021-2027/conditie-favorizanta/sncisi_19-iulie.pdf

Ministry of Research, Innovation and Digitalization (2021). Framework Document on the National Strategy for Research, Innovation and Smart Specialization 2021-2027, November, https://www.poc.research.gov.ro/uploads/2021-2027/conditie-favorizanta/sncisi-draft.pdf

Montagna, M., Gabriele Torri, G. & Covi, G. (2020). On the origin of systemic risk, Working Paper Series No. 2502, December, European Central Bank, https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2502~675f29f90c.en.pdf

National Cyber Security Center, Building a Security Operations Centre (SOC) , United Kingdom of Great Britain and Northern Ireland, https://www.ncsc.gov.uk/collection/building-a-security-operations-centre/onboarding-systems-and-log-sources/threat-modelling

Orlando, A. (2021). Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk, https://www.mdpi.com/2227-9091/9/10/184/htm

Romanian Government (2021). Romania's Security Strategy for the period 2022-2027, https://legislatie.just.ro/Public/DetaliiDocumentAfis/250235

Romanian Government (2021). Action Plan for implementing Romania's Security Strategy for the period 2022-2027, https://legislatie.just.ro/Public/ DetaliiDocumentAfis/ 250236

Romanian Government (2020). Romania's National Defense Strategy for the period 2020-2024, Bucharest, https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala de_ Aparare a_Tarii_ 2020_ 2024.pdf

Romanian Government (2018). Romania's National Strategy for Sustainable Development 2030, https://dezvoltaredurabila.gov.ro/strategia-nationala-pentru-dezvoltarea-durabila-a-romaniei-2030-i

Romanian Government (2021). The National Recovery and Resilience Plan for Romania, Ministry of European Investments and Projects, October, https://mfe.gov.ro/pnrr/

Senabre, S., Soto, I. & José Munera, J. (2021), Strengthening the cyber resilience of the financial sector. Developments and trends, Banco de Espana, https://www.bde.es/f/webbde/Secciones/Publicaciones/InformesBoletinesRevistas/InformesEstabilidadFinancera/21/5_Ciberresiliencia_FSR41.pdf

Şcheau, M. C. (2018). Informatics criminality regarding financial transfers, Economica Publishing, Bucharest, ISBN 978-973-709-871-9

Stoneburner, G.; Goguen, A.; Feringa, A. (2002). Risk Management Guide for Information Technology Systems, National Institute of Standards

and Technology, Special Publication 800-30, July, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf

SWIFT. Reducing risk and increasing resilience in RTGS payment systems, https://www.swift.com/swift-resource/4001/download?language=en

Vanini, P.; Rossi, S.; Zvizdic, E.; Domenig, T. (2023). Online payment fraud: from anomaly detection to risk management, https://jfin-swufe.springeropen.com/articles/10.1186/s40854-023-00470-w

World Bank Group (2021). Considerations and Lessons for the Development and Implementation of Fast Payment Systems, September, https://fastpayments.worldbank.org/sites/default/files/2021-11/Fast%20Payment%20Flagship_Final_Nov%201.pdf

World Bank Group (2021), Financial Sector's Cybersecurity: A Regulatory Digest, 6th Edition, Financial Sector Advisory Center (FinSAC), August, https://thedocs.worldbank.org/en/doc/3c28bd048d78efd27744987253e2c44a-0430012021/related/CybersecDigest-v6-FINAL-ed.pdf

World Economic Forum (2016). Understanding Systemic Cyber Risk, Global Agenda Council on Risk & Resilience, October, https://www3. weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf

World Economic Forum (2022). The Global Risks Report 2022, 17th Edition, Insight Report, ISBN: 978-2-940631-09-4, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

World Economic Forum (2019). The Global Risks Report 2019, 14th Edition, ISBN: 978-1-944835-15-6

World Economic Forum (2021). Beneath the surface. Technology-driven Systemis Risks and the Continued Need for Innovation, Part of the Future of Financial Services series, prepared in collaboration with Deloitte, October, https://www3.weforum.org/docs/WEF_Technology_Innovation_and_Systemic_Risk_2021.pdf