Cybersecurity Risks in Digitized Capital Markets: A Comparative Regulatory Analysis of Operational Resilience, Disclosure, and Market Integrity

Akomolehin Francis Olugbenga

Department of Finance, College of Management & Social Science Afe Babalola University, Ado - Ekiti Ekiti

DOI: https://doi.org/10.51244/IJRSI.2026.1307000252

Received: 28 July 2026; Accepted: 03 August 2026; Published: 10 August 2026

ABSTRACT

The digitization of capital markets has increased efficiency, connectivity, and innovation, but it has also transformed cybersecurity from an institution-specific technical concern into a systemic threat to market integrity and financial stability. This study evaluates the adequacy and coherence of cybersecurity regulation in digitized capital markets. It employs qualitative policy analysis, doctrinal review, and comparative analysis of the United States Securities and Exchange Commission framework, the European Union's Digital Operational Resilience Act, and IOSCO/CPMI-IOSCO standards. Regulatory documents and scholarly evidence covering 2020–2026 are assessed through directed content analysis and a comparative matrix spanning governance, incident reporting, disclosure, resilience testing, third-party risk, business continuity, enforcement, and systemic resilience. The findings reveal partial regulatory convergence but persistent structural fragmentation. The United States prioritizes disclosure and investor protection; the European Union adopts a broader operational-resilience model; and international standards emphasize financial-market infrastructures, coordination, and systemic stability. Major deficiencies include weak integration between disclosure and resilience requirements, uneven oversight of critical technology providers, inconsistent incident definitions and reporting timelines, limited cross-border enforcement, and inadequate treatment of contagion and market outages. The study proposes a multilayered regulatory model that aligns entity-specific obligations with harmonized reporting, proportionate disclosure, direct oversight of critical third parties, coordinated recovery planning, and market-wide resilience testing. Such integration is essential for protecting investors, preserving market continuity, and containing systemic cyber risk.

Keywords: Cybersecurity risk; Digitized capital markets; Operational resilience; Regulatory governance; Market integrity; Systemic risk.

INTRODUCTION

Background to the Study

However, the digitization of capital markets has drastically changed the structure, operations, and risks of modern financial systems. The increasing digitization of trading facilities, clearing and settlement structures, broker-dealers, asset managers, and issuers involves interconnections of various digital technologies, ranging from cloud computing solutions, algorithmic trading tools, distributed ledger technologies, and real-time data analytics (Buttigieg & Brunelli Zimmermann, 2024; International Organization of Securities Commissions [IOSCO], 2024). While digitization improves efficiency, liquidity, and cross-border integration of markets, it expands the cybersecurity attack surface of the entire capital market ecosystem (Buttigieg & Brunelli Zimmermann, 2024; IOSCO, 2024).

The principal cybersecurity risks in digitized capital markets arise from systemic third-party dependencies, algorithmic and application programming interface vulnerabilities, and severe operational disruptions. Capital-

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

market institutions increasingly depend on a concentrated group of cloud-service providers, data vendors, software firms, and network operators. Although these arrangements improve scalability and reduce operating costs, they create common points of failure. A successful attack or prolonged outage affecting one critical provider could simultaneously impair trading venues, broker-dealers, asset managers, clearinghouses, and securities depositories, allowing cyber risk to spread across interconnected markets.

Algorithmic trading systems, real-time market-data feeds, and application programming interfaces also introduce vulnerabilities capable of undermining market integrity. Malicious actors may exploit weak access controls, corrupt data inputs, manipulate automated orders, or interfere with execution algorithms. Such attacks could generate abnormal trading patterns, artificial price movements, liquidity deterioration, or flash-crash conditions before market operators can intervene.

Operational disruption constitutes a further systemic threat. Ransomware, distributed denial-of-service attacks, destructive malware, and data corruption can suspend trade execution, clearing, settlement, custody, disclosure, and market-data services. When these functions remain unavailable, unsettled obligations accumulate, liquidity pressures increase, and investor confidence declines. Cybersecurity risk in digitized capital markets should therefore be understood as a market-wide governance and financial-stability concern rather than merely an internal information-technology problem. Effective regulation must combine third-party oversight, algorithmic and API security, resilience testing, incident reporting, coordinated recovery arrangements, and carefully designed public disclosure requirements.

Regulators around the world have responded to the evolution of the cybersecurity risks faced by capital markets by adapting their approach toward cybersecurity governance. For example, the SEC has increased emphasis on cybersecurity risk disclosure, as well as strengthened the role of corporate boards in managing these risks, imposing obligations for prompt reporting of material cybersecurity incidents and establishing governance procedures (U.S. Securities and Exchange Commission [SEC], 2023). At the same time, EU regulators have introduced a comprehensive regulatory framework of operational resilience requirements to cover all aspects of the issue, including cybersecurity, with the adoption of DORA (Buttigieg & Brunelli Zimmermann, 2024). Finally, international standard-setters have focused increasingly on cybersecurity risks at the level of financial market infrastructures (FMI), recognizing the need to protect market continuity against systemic cyber risks (Buttigieg & Brunelli Zimmermann, 2024; IOSCO, 2024).

Thus, although cybersecurity governance in capital markets has significantly progressed, the regulation of these risks continues to differ greatly between countries, with various regulatory approaches focusing on disclosure, resilience, and systemic cybersecurity concerns.

Research Problem

The importance of cybersecurity in financial regulation has risen significantly, though it is apparent that the current regulatory responses to cyber-related risks suffer from certain inconsistencies. There is a continuous gap in perception of cybersecurity either as a disclosure matter that aims at informing investors or as a resilience matter focused on continuity and stability of operation (see Buttigieg & Brunelli Zimmermann, 2024). While disclosure-focused regulation, like the framework adopted by SEC, provides greater transparency, it does not necessarily solve the problem of operational vulnerabilities that can lead to disruptions (SEC, 2023). On the other hand, resilience-focused legislation, including DORA, includes stronger risk management mechanisms but brings up questions concerning coordination of supervision and implementation of the regulation across borders (Buttigieg & Brunelli Zimmermann, 2024).

Additionally, increasing interdependence among the participants of capital markets due to digital infrastructure and the use of services provided by third parties creates conditions that contribute to systemic risks, which are beyond the scope of firm-centric regulatory frameworks (Buttigieg & Brunelli Zimmermann, 2024). According to empirical evidence, cyberattacks can spread throughout financial networks and thus pose threats to systemic risk and the outcomes of market operations, including liquidity and valuation (Kotidis & Schreft, 2025; Zhang & Wong, 2025). The current regulatory frameworks focus on regulating issuers, intermediaries, and market infrastructures separately.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

Therefore, there is a need for thorough analysis of how current regulatory regimes perceive and respond to cybersecurity risks associated with digitized capital markets and if these approaches are adequate enough to ensure market integrity and systemic resilience.

Research Questions

This study is guided by the following research questions:

What are the key cybersecurity risks associated with the digitization of capital markets?

How do major regulatory frameworks—particularly in the United States, European Union, and international standard-setting bodies—address these risks?

What are the main gaps, overlaps, and inconsistencies in current regulatory responses to cybersecurity in capital markets?

How can regulatory frameworks be enhanced to better align cybersecurity governance with market integrity and systemic resilience objectives?

Research Objectives

The primary objective of this study is to critically evaluate the adequacy of regulatory responses to cybersecurity risks in digitized capital markets. To achieve this aim, the study seeks to:

Identify and analyze the principal cybersecurity risks arising from the digitization of capital markets;

Examine and compare key regulatory frameworks governing cybersecurity in the United States, European Union, and at the international level;

Assess the strengths and limitations of these regulatory approaches in addressing firm-level and systemic cyber risks;

Propose policy recommendations aimed at enhancing regulatory coherence, effectiveness, and resilience in capital markets.

Scope of the Study

This research adopts a comparative approach in analyzing policy aspects, focusing mainly on three core regulation areas: United States, European Union, and international standards-setting institutions, especially those formulated by IOSCO. The scope of this study covers only cybersecurity threats in the capital markets sector, which includes publicly traded companies, market participants (such as brokers and asset management firms), and financial market infrastructure organizations (like stock exchanges, central counter-parties, and securities depositories).

This research focuses on regulatory activities between 2020 and 2026, capturing the most recent policy changes related to cyber risk management. This research will not undertake any technical assessment of cyber security tools, as its scope is confined to the policy perspective of cyber risk governance. Finally, although this research takes into consideration international views, it does not attempt a comprehensive coverage of all regulatory regimes but instead focuses on key examples.

Significance of the Study

In conclusion, this study has made a number of important contributions to scholarly literature and practice. Firstly, this paper contributes to extant research literature through bringing together two distinct research fields: cybersecurity disclosure and resilience. Whereas previous studies have considered the impact of cybersecurity disclosures on investor behavior, firm governance, and stock prices (Huang & Murthy, 2024; Gao & Calderon,

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

2025), little empirical research has attempted to understand the extent to which regulatory frameworks incorporate consideration of the systemic aspects of cyber risk.

Secondly, this paper provides a comparative view of regulation in cybersecurity governance that allows one to identify similarities and differences between major cybersecurity governance models, thus offering valuable insights into the advantages and disadvantages of extant regulatory frameworks and pointing at areas where harmonization of different models may be required.

Finally, the study carries practical significance for decision-makers in capital markets by revealing gaps in existing regulatory mechanisms in light of increasing cyber risks. Given the need to create robust cybersecurity regulations in order to foster operational continuity and systemic stability, this study will be useful for developing new and improved regulatory strategies for cyber risks in digitized capital markets.

The bottom line is that cybersecurity regulation deserves greater attention from decision-makers as a crucial aspect of capital market governance.

LITERATURE REVIEW

Conceptual Review

This section synthesizes contemporary scholarship on cybersecurity risks in digitized capital markets through an integrated analytical lens. Rather than treating cybersecurity as a purely technical or firm-level issue, the literature increasingly situates it at the intersection of market structure, governance, and systemic stability. Four interrelated themes emerge: the technological transformation of capital markets and its cyber implications; cybersecurity as a disclosure and governance concern; cybersecurity as an operational-resilience and systemic-risk issue; and evolving regulatory responses alongside persistent tensions.

Digitization of Capital Markets and Expanding Cyber-Attack Surfaces

Firstly, the digitalization of capital markets has enhanced efficiency, speed, and globalization, but has introduced elaborate cyber vulnerabilities integrated within the underlying technological platforms. Automated algorithmic and high-frequency trades, for example, are characterized by high-speed transaction processing and execution, which makes them vulnerable to manipulation or disruption. Artificial Intelligence-based and Machine Learning approaches in trading strategies have further complicated security issues, since the opaque processes involved may make such systems hard to secure and monitor (Gao & Calderon, 2025).

Moreover, the reliance on cloud computing and outsourced Information Communication Technology (ICT) services is an emerging issue. There is an increased use of few cloud service providers for the provision of services and products in financial systems, leading to operational concentration risk or single points of failure. According to Buttigieg and Brunelli Zimmermann (2024), such practices have made financial systems highly vulnerable to cyber risks, especially due to disruptions in more than one institution at a time.

Additionally, there is a trend towards greater API and real-time data connectivity that allows the smooth integration of participants in capital markets. This has led to enhanced efficiency in trading and other operations, although it opens up opportunities for lateral attack propagation across the financial ecosystem through many points of intrusion (IOSCO, 2024).

There have been recent efforts that show how the interconnectivity of these issues makes them highly systemic. For instance, Kotidis and Schreft (2025) present evidence about how cyberattacks propagate through FMI via their dependence on common service providers. This has the potential to increase cyber-contagion effects across the financial system, making it highly vulnerable to cyber threats. Thus, the concept of FMI resilience assumes a prominent role here, since disruptions to critical FMI will lead to cascading consequences across all capital markets. Clearly, the expansion of the cyberattack surface through digitization goes hand-in-hand with making cybersecurity an inherently networked and systemic issue. The interconnectedness of cybersecurity risks in digitized capital markets is captured in Figure 1 below, where some of the important ecosystem actors and dependencies related to cyber risks are presented.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

Figure 1: Capital Market Cyber Risk Ecosystem Map.

This figure illustrates the interconnected ecosystem of cybersecurity risk in capital markets, highlighting the dynamic relationships among key components: issuer disclosure, operational resilience, third-party risk governance, infrastructure oversight, and regulatory enforcement. It demonstrates how cyber risks originate, propagate, and amplify across interconnected market participants, infrastructures, and service providers, emphasizing the systemic nature of cybersecurity threats in digitized financial systems.

Source: Author's conceptualization based on Buttigieg and Brunelli Zimmermann (2024), Huang and Murthy (2024), Gao and Calderon (2025), Kotidis and Schreft (2025), and International Organization of Securities Commissions (2024).

Cybersecurity as a Market-Governance and Disclosure Issue

An expanding literature stream has treated cybersecurity from the perspective of corporate governance and financial disclosure in capital markets. In such an approach, cybersecurity risk is viewed as a source of information asymmetries between investors and corporate entities that affect investment decisions and the efficiency of capital markets.

Cyber-risk disclosures have become one of the key aspects of regulation and academic research. According to Huang and Murthy (2024), high-quality, detailed, and timely cybersecurity risk disclosures are vital for forming investors' opinions and making accurate investment choices. Similarly, Amani et al. (2025) highlight the importance of transparent cyber-risk exposure disclosure to decrease the problem of information asymmetry.

However, at the same time, corporate governance plays an essential role in shaping disclosure decisions made by companies. For instance, Gao and Calderon (2025) found that having good cybersecurity governance frameworks, such as separate boards and positions related to information protection, positively impacts disclosures and helps form better information environments.

Market effects of cybersecurity risk and disclosure are also thoroughly researched. Empirical evidence demonstrates that cyber risk can be a factor affecting firm value and stock liquidity when investors think that a firm is exposed to such risks and does not practice proper management (Zhang & Wong, 2025). Moreover, mandatory disclosure systems may affect insider trading activities and market responses to cybersecurity issues (Chen et al., 2025).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

However, the disclosure-based framework of cybersecurity risk management has some drawbacks associated with its inability to ensure that all measures are taken to prevent and manage potential threats and risks. That is why nowadays, the significance of operational cybersecurity and systemic risk is increasingly recognized.

Operational Resilience and Systemic Cyber Threats

Cybersecurity risk in digitized capital markets extends beyond data confidentiality to the continued availability, integrity, and reliability of critical market functions. Trading, price discovery, clearing, settlement, custody, market-data distribution, and regulatory reporting now depend on interconnected information and communication technology systems. A serious cyber incident affecting any critical component can interrupt transactions, impair liquidity, delay settlement obligations, and weaken investor confidence. Operational resilience therefore requires capital-market institutions to anticipate, withstand, respond to, recover from, and adapt to cyber incidents without allowing critical services to deteriorate beyond acceptable limits (Buttigieg & Brunelli Zimmermann, 2024; IOSCO, 2024).

A major systemic threat arises from cloud and third-party dependence. Exchanges, intermediaries, asset managers, issuers, and financial market infrastructures increasingly outsource data storage, processing, software, connectivity, and cybersecurity services to external providers. Where several institutions rely on the same vendor, a breach or outage at that provider becomes a common point of failure. The resulting disruption may spread simultaneously across multiple market participants rather than remain confined to one institution. This concentration risk is particularly serious when firms lack effective exit arrangements, interoperable backup systems, data portability, or substitutable providers. DORA responds through requirements covering ICT risk management, contractual controls, registers of third-party arrangements, concentration-risk assessment, resilience testing, incident reporting, and oversight of designated critical ICT providers. These measures reflect a regulatory shift towards treating third-party dependence as a potential source of system-wide disruption rather than a routine outsourcing matter (European Union, 2022).

Algorithmic trading systems, application programming interfaces and real-time data feeds constitute a second category of systemic vulnerability. Malicious actors may compromise authentication controls, inject corrupted market data, manipulate automated instructions, or exploit weaknesses in trading algorithms. Because automated systems execute decisions at high speed, a compromised signal can produce rapid order imbalances, abnormal price movements, liquidity withdrawal or disorderly trading before manual intervention becomes possible. The risk becomes systemic when interconnected institutions respond automatically to the same corrupted data or market signal. Effective governance should therefore include secure software development, API authentication, data-integrity validation, algorithm testing, real-time surveillance, kill switches and coordinated market-wide response procedures.

Ransomware and other extortion-based attacks present a third operational threat because they target the availability of essential systems and data. An attack on an exchange, central counterparty, securities depository, broker or shared service provider can suspend trading, freeze clearing and settlement processes, prevent access to collateral records, and delay regulatory reporting. Prolonged disruption can produce unsettled obligations, liquidity shortages, counterparty uncertainty and cascading losses across connected institutions. Consequently, resilience frameworks should require segregated backups, recovery-time objectives, crisis simulations, communication protocols, alternative processing arrangements and coordinated recovery plans for critical market services.

Regulatory responses nevertheless differ in emphasis. DORA establishes prescriptive obligations concerning ICT risk management, incident reporting, resilience testing and third-party oversight. In contrast, the U.S. Securities and Exchange Commission requires public companies to disclose material cybersecurity incidents, generally within four business days after determining materiality, and to report periodically on cybersecurity risk management, strategy and governance (SEC, 2023). While disclosure improves investor information, it does not by itself require specific technical defences or guarantee operational continuity. IOSCO and CPMI-IOSCO complement these approaches by stressing market-outage preparedness, recovery of financial market infrastructures, information sharing and coordinated responses to market-wide disruption. An effective

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

framework must therefore integrate operational resilience, third-party oversight, market-integrity controls and appropriately calibrated disclosure rather than treat them as separate regulatory concerns.

Regulatory Responses and Unresolved Tensions

Regulators have responded by developing a range of different frameworks that aim at bolstering cyber resilience in capital markets. The response strategies employed by different regulators are guided by varying ideologies, leading to some form of divergence and convergence of efforts.

On one hand, the U.S. Securities and Exchange Commission (SEC) adopted a disclosure-based model where publicly traded companies are required to reveal any cybersecurity events that are deemed material along with their associated risk management and governance strategies (SEC, 2023). The disclosure-based model relies on investor protection and is aimed at reducing information asymmetry and increasing market efficiency.

On the other hand, the European Union has passed the Digital Operational Resilience Act (DORA), which represents a much more prescriptive regulatory regime based on the concept of operational resilience. The DORA regulation combines ICT risk management, incident reporting, resilience testing, and control over critical third parties into a single legal framework (Buttigieg & Brunelli Zimmermann, 2024). This trend indicates a shift towards cybersecurity being considered as a cross-sectoral systemic challenge.

At the international level, IOSCO and CPMM-IOSCO have developed principles and guidance documents that focus on cyber resilience, including market infrastructures (IOSCO, 2024).

It should be noted, however, that there are several unresolved challenges in this field. Firstly, there is an inherent trade-off between transparency and cybersecurity, as more information disclosed to the public raises the likelihood of being exploited by malicious actors. Secondly, proportionality and appropriateness of regulation should be taken into account, particularly when it comes to smaller players unable to implement elaborate resilience measures. Thirdly, fragmented regulatory practices across sectors and countries might result in inconsistencies and possible gaps in enforcement.

As can be seen from above, there is a need for a new approach to regulating cybersecurity issues in capital markets that will balance between the elements mentioned.

Theoretical Framework

To understand the cybersecurity risks of the digitized capital markets as an object of academic research, one has to adopt a multi-theoretical approach. While there is no single theoretical perspective sufficient to describe the complexity of the issues involved, combining agency, stakeholder, systems (network), and regulatory theories allows us to obtain a comprehensive picture that is capable of explaining the origin of cyber risks and the reasons behind the evolving regulatory response.

In this sense, agency theory presents a foundational basis for explaining why cybersecurity becomes increasingly important to capital markets by referring to the phenomenon of information asymmetry between firm managers and investors. In the domain of cybersecurity, managers possess information regarding the cybersecurity policies, incident exposures, and potential weaknesses of their organization, while investors rely solely on the information that has been reported. As a result, incentives for underreporting exist because any disclosure may harm the organization's valuation and/or reputation. To eliminate this incentive, regulators enforce mandatory disclosure requirements to minimize information asymmetry. According to empirical research, cybersecurity disclosures have significant effects on the behavior and decisions made by investors, proving the applicability of agency theory in this context (Huang & Murthy, 2024). Likewise, the governance practices (e.g., board supervision) and the structure of the organizational control affect cybersecurity disclosures. For instance, Gao and Calderon find that cybersecurity governance structures improve cybersecurity disclosures and reduce agency costs (2025). Nevertheless, while agency theory provides a good explanation for the necessity of mandatory disclosure of cybersecurity risks, it does not provide a solution to problems that go beyond disclosure and involve broader regulatory concerns.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

In contrast, stakeholder theory acknowledges that cybersecurity risk concerns more than just shareholders. Indeed, in digitized capital markets, the disruption of operations due to cyber incidents may negatively affect not only firm performance but also market functions, investor confidence, and financial stability. Thus, a wider perspective on cybersecurity is needed to justify the governance of the cybersecurity risks that pose a threat not only to individual firms but also the financial system in general. The stakeholder perspective suggests that cybersecurity should be considered as a public problem with externalities, requiring collective management that will prevent the risk from harming other stakeholders. Consistent with this perspective, EU emphasizes the importance of developing operational resilience in digitized capital markets. Buttigieg and Brunelli Zimmermann demonstrate how operational resilience helps firms deal with cyber risks that threaten the stability of the financial system (2024). In this sense, stakeholder theory offers an adequate explanation for the necessity of shifting cybersecurity regulations away from mere disclosure and toward ensuring resilience of the capital markets.

While agency and stakeholder theories allow us to explain the importance of governance measures, systems theory (or, in this case, financial network theory) provides important insight into the systemic nature of the cybersecurity risk. The financial system is now characterized by a high degree of interconnectivity that is facilitated by technological advancements. Thus, cyber risk becomes a networked risk and, depending on the nature of the incident, a threat to the system as a whole. This is due to the increasing use of third-party vendors in financial transactions, providing channels for contagion (Kotidis & Schreft, 2025). As a result, cybersecurity in digitized capital markets needs to account for the systemic nature of the risk and be based not on the idea of isolated entities' survival but the sustainability of the system as a whole.

Finally, regulation theory provides a framework for explaining the need for and nature of cybersecurity regulations in digitized capital markets. In terms of regulation theory, regulation can be seen as a public intervention meant to overcome market failure caused by externalities and other types of asymmetries between various parties. Indeed, cybersecurity risk fits the definition of market failure well: the cost incurred by firms in protecting themselves against cyber risk makes it unlikely for them to invest in cybersecurity adequately, while, once realized, cybersecurity risk poses significant hazards to market stability. Thus, regulators introduce requirements that force organizations to disclose their vulnerabilities and invest more in cybersecurity management. However, regulation theory also draws attention to the problem of fragmentation of cybersecurity regulations across jurisdictions and inconsistency between them. Such fragmentation is caused by the difference in objectives pursued by various regulatory authorities and may become problematic for achieving cybersecurity goals.

Overall, this brief theoretical overview indicates that the combination of agency, stakeholder, network, and regulatory theories allows for the comprehension of complex issues of cybersecurity management in digitized capital markets. Agency theory explains why regulators introduce disclosure measures and governance mechanisms to reduce information asymmetry, while stakeholder theory helps comprehend why the scope of cybersecurity regulation is expanding and includes elements that cannot be explained using only agency theory. Network theory allows us to recognize the importance of systemic perspective on cyber risk, while regulation theory helps understand the logic behind the evolution of the regulatory regime and the problems associated with it.

By integrating these theoretical perspectives, we can construct a multi-dimensional framework for assessing the current situation in the sphere of cybersecurity management in digitized capital markets. Moreover, it can help us identify gaps in existing regulations and suggest improvements.

Analytical Framework

As indicated above, the analysis and comparative assessment of cybersecurity regulations in digitized capital markets rely on the selected theoretical framework. The analytical framework employed here offers a structured perspective for evaluating cybersecurity risk mitigation policies in regulatory regimes. The framework draws from three major theoretical perspectives, namely agency theory, systems theory, and regulatory theory, to consider cybersecurity risk as a multidimensional phenomenon created by the interaction of disclosure, resilience, governance, and systemic oversight.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

While cybersecurity risk tends to be treated mainly as a technical concept, the chosen framework perceives cyber risk in terms of regulatory design and effectiveness as exercised at various layers of the market infrastructure. More specifically, the framework models cyber risk in the capital market as a complex phenomenon that depends on five interrelated regulatory aspects: disclosure regulation, operational resilience, third-party risk governance, infrastructure oversight, and enforcement capacity.

According to Buttigieg and Brunelli Zimmermann (2024), disclosure regulation is one of the major forms of cyber risk regulation in financial markets that aims to increase transparency in relation to material cyber events, cybersecurity governance structures, and cyber risk management activities. Although empirical evidence shows that such regulations affect investors' perception, market reaction, and even firm valuation (Huang & Murthy, 2024; Gao & Calderon, 2025), disclosure does not eliminate cyber risk without proper operational controls.

The next dimension of cyber risk regulation is operational resilience, which refers to the ability of a financial entity to anticipate, withstand, respond to, and recover from cyber risk incidents. As per Buttagieg and Brunelli Zimmermann (2024), regulatory regimes have increasingly moved toward the concept of operational resilience due to the growing sophistication of cyberattacks in recent years. According to IOSCO (2024), effective cyber risk regulation should cover incident response management, internal control structures, business continuity planning, and resilience testing.

The third dimension of cyber risk regulation concerns third-party risk governance. It is related to the growing tendency of financial entities to delegate important activities to third parties, which creates new cyber vulnerabilities. In today's digitized environment, cloud infrastructure, ICT services, and data providers are essential for the operations of most firms. Moreover, Kotidis and Schreft (2025) show that cyberattacks can propagate through financial markets based on the dependence between firms. Therefore, the effective governance of third-party relationships is essential for mitigating cyber risk.

Infrastructure oversight is another critical aspect of cyber risk regulation, which entails the monitoring and control of FMIs. FMIs, such as exchanges and clearinghouses, are essential elements in financial markets that may contribute to systemic risk through their interactions with other market participants. Disruptions in the work of an FMI may result in the interruption of market activities and even market outages (IOSCO, 2024).

Finally, enforcement capacity is the last dimension of cyber risk regulation and is a kind of crosscutting aspect, since it determines the effectiveness of all other regulatory regimes. The enforcement capacity involves supervisory and compliance activities aimed at enforcing regulatory requirements. Differences in enforcement capacity across jurisdictions may have a dramatic effect on the effectiveness of cybersecurity regulations in a certain jurisdiction.

The five dimensions of cyber risk regulation are evaluated based on five analytical criteria, which include scope, substance, timeliness, supervision and enforcement, and systemic orientation. Scope relates to the scope of regulations and concerns such entities as issuers, intermediaries, and FMIs. Substance involves the analysis of regulatory substance or depth. It is assessed in terms of regulatory requirements for incident response, testing, governance, etc. Timeliness covers issues of timeliness of disclosure. The next criterion concerns supervisory and enforcement mechanisms, while the last criterion measures systemic orientation of regulatory regimes.

This analytical structure makes it possible to compare various cybersecurity regulatory regimes by assessing them in relation to specific dimensions and criteria. For instance, one may compare disclosure regimes that focus on the transparency aspect and investor protection and regimes based on the principle of operational resilience aimed at improving preparedness to cyber risk. At the same time, international standards pay much attention to systemic orientation, but often they lack mandatory requirements and enforcement.

Thus, the chosen framework allows analyzing and comparing cybersecurity regulations by taking into account five essential dimensions: disclosure, resilience, governance of third parties, infrastructure oversight, and enforcement. Moreover, each of these dimensions can be evaluated using five criteria: scope, substance,

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

timeliness, supervision/enforcement, and systemic orientation. This framework makes it possible to identify structural weaknesses in cybersecurity regulatory regimes and offer policy recommendations concerning regulatory improvement.

METHODOLOGY

For the current study, a qualitative policy analysis, in combination with a comparative analysis of regulatory systems, is applied to examine the adequacy and consistency of cybersecurity governance in capital markets that have been digitalized. In line with the normative and institutional features of the research question at hand, the methodological approach involves a combination of legal doctrinal analysis with a structured policy evaluation to allow for a descriptive and critical evaluation of the respective regulatory regimes.

Research Design

A combination of doctrinal and comparative as well as policy-analytic research design is utilized for the purpose of conducting this study. As a part of doctrinal research, legal and regulatory documents dealing with cyber security in capital markets will be analyzed in terms of their structure, range and substantive content. These legal materials include formal rules as well as regulatory guidelines issued by both domestic and international authorities.

As a part of comparative research, commonalities, differences and distinctions in terms of approaches to regulating cyber risks will be identified across jurisdictions. By conducting a comparative analysis between U.S., EU countries as well as international standard setters, the study will be able to show different approaches taken by these jurisdictions in terms of regulating cyber risks in capital markets.

Finally, as a part of policy analytic aspect of the research, not only these legal and regulatory frameworks will be described but also evaluated in terms of their adequacy to regulate cyber risks effectively. In particular, the research will show whether these regulatory efforts reflect multiple dimensions of cyber risks.

Data Sources

The review considers the following main types of data sources: regulatory primary information and academic secondary data. Regulatory primary data are authoritative information sources that influence the cybersecurity governance of capital markets. Among these, the following sources are considered: the final rule of the U.S. Securities and Exchange Commission on the cybersecurity risk management, strategy, governance, and incident disclosure (SEC, 2023); the EU Digital Operational Resilience Act (DORA), as well as other documents by the European Supervisory Authorities (ESAs) in the framework of DORA, specifically the European Securities and Markets Authority (ESMA); and international frameworks such as the IOSCO reports on market outages and risk outlooks, along with the CPMI-IOSCO guidance on cyber resilience of financial market infrastructures. These sources are selected due to their recent influence on regulatory actions on cybersecurity between 2020 and 2026. Academic secondary sources refer to articles that have been published within the period of 2020-2026 and have been reviewed and published in academic journals. Such articles deal with cybersecurity disclosure, cyber risk governance, effects of cybersecurity threats on financial markets, and systemic cyber risks. Examples of such publications include Huang and Murthy's research on the role of cybersecurity disclosures on investor behavior and firm valuation (2024), Gao and Calderon's article on the propagation of cyber risks through the network of financial institutions (2025), and Buttigieg and Brunelli Zimmermann's study of digital operational resilience within the framework of financial regulation (2024).

Case-Selection Logic

The case-selection strategy is guided by a multi-level regulatory architecture and a cross-jurisdictional comparative framework, designed to capture the complexity of cybersecurity governance in capital markets.

At the first level, the study distinguishes among three categories of market participants:

i. Issuers, representing publicly listed companies subject to disclosure obligations;

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

ii. Market intermediaries, including broker-dealers, asset managers, and investment firms that facilitate trading and capital allocation;

iii. Financial market infrastructures (FMIs), such as exchanges, central counterparties, and securities settlement systems, which are critical to market functioning and systemic stability.

This classification reflects the heterogeneous nature of cyber risk exposure and regulatory obligations across different segments of the capital market ecosystem.

At the second level, the study compares three major regulatory layers:

I. The United States, represented primarily by the SEC's cybersecurity disclosure regime;

II. The European Union, represented by DORA and associated supervisory frameworks;

III. International standards, particularly those developed by IOSCO and CPMI-IOSCO, which provide principles and guidance for global coordination and systemic resilience.

This selection is based on the influence, diversity, and complementarity of these regulatory regimes. The United States and European Union represent two leading but distinct regulatory models—one disclosure-oriented and the other resilience-oriented—while international standards provide a benchmark for assessing global coherence and best practices.

By combining entity-level and jurisdictional dimensions, the case-selection logic enables a comprehensive analysis of how cybersecurity risks are addressed across different layers of the financial system and regulatory hierarchy.

Analytical Technique

The study employs directed qualitative content analysis complemented by a comparative legal matrix to systematically evaluate regulatory frameworks. Directed content analysis is particularly suitable for theory-informed research, as it allows predefined categories—derived from the conceptual framework—to guide the coding and interpretation of textual data.

Regulatory documents are analyzed and coded across eight key dimensions:

Governance, including board oversight, risk management structures, and accountability mechanisms;

Incident reporting, encompassing requirements for identifying, classifying, and reporting cyber incidents to regulators;

Disclosure, focusing on public reporting obligations and transparency requirements;

Testing, including resilience testing, penetration testing, and scenario analysis;

Third-party risk, addressing outsourcing, vendor management, and oversight of critical service providers;

Business continuity, covering recovery planning, redundancy, and operational resilience;

Enforcement, including supervisory mechanisms, compliance monitoring, and sanctions;

Systemic resilience, reflecting the extent to which frameworks address contagion, interdependencies, and market-wide disruptions.

These dimensions are further aligned with the five evaluative criteria outlined in the conceptual framework—scope, substance, timeliness, supervision and enforcement, and systemic orientation—allowing for a structured and comparative assessment of regulatory regimes.

The comparative legal matrix serves as a tool for organizing and synthesizing findings across jurisdictions and entity types. It enables the identification of patterns, gaps, and overlaps in regulatory approaches, as well as the evaluation of their relative strengths and weaknesses. By systematically mapping regulatory provisions against analytical criteria, the study moves beyond descriptive comparison to provide a nuanced and evidence-based assessment of cybersecurity governance in digitized capital markets.

This methodological approach ensures analytical transparency, conceptual consistency, and comparative rigor, thereby enhancing the validity and scholarly contribution of the study.

The integrated conceptual framework guiding this study is illustrated in Figure 2, which highlights the interaction between key regulatory dimensions and their operational proxies in shaping cybersecurity risk in capital markets.

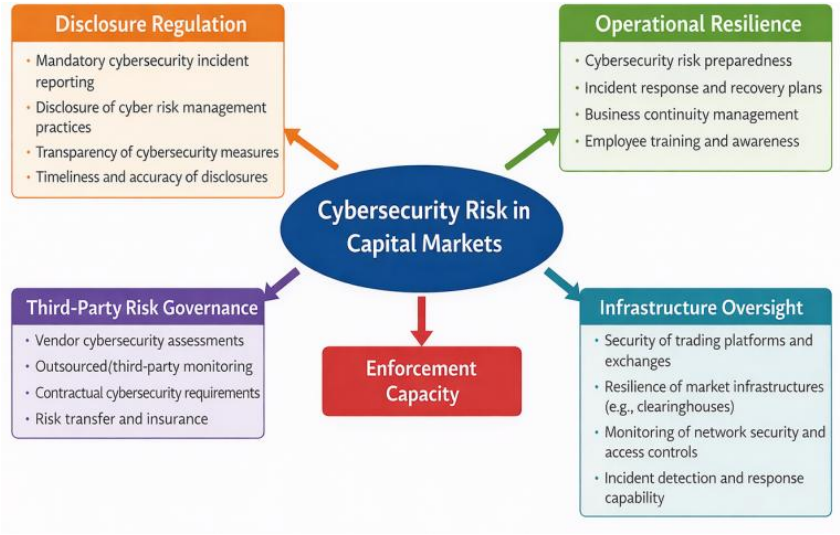

Figure 2: Conceptual Framework of Cybersecurity Risk in Digitized Capital Markets.

This figure illustrates cybersecurity risk as a multidimensional construct shaped by disclosure regulation, operational resilience, third-party risk governance, infrastructure oversight, and enforcement capacity. Each dimension is operationalized through key regulatory proxies, reflecting the interaction between transparency, resilience, and systemic oversight in capital markets.

Source: Author's conceptualization based on Huang and Murthy (2024), Gao and Calderon (2025), Buttigieg and Brunelli Zimmermann (2024), Kotidis and Schreft (2025), and IOSCO (2024)

Regulatory Mapping and Findings

In this part, I present the comparative discussion about the main regulatory strategies for dealing with cybersecurity issues in the digitized capital markets based on the framework discussed in the previous section. In this regard, it is clear that there is a significant difference between the regulatory strategies implemented in different places in terms of their philosophy and structure. While the US focuses on disclosure strategy, EU is concerned with operational resilience, and international standard-setters give importance to systemic stability and coordination.

United States: Disclosure-Led Response

The regulatory position of the United States on cybersecurity within capital markets is mainly disclosure-based, with the Securities and Exchange Commission (SEC) considering cybersecurity to be a material risk that should be disclosed to the investors. The recent development of a regulation issued by the SEC in 2023, concerning cybersecurity risk management, strategy, governance, and incident disclosure, represents a significant progress in this regard since it mandates public companies to disclose relevant data related to cybersecurity (SEC, 2023).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

Among the elements of the new rule is the requirement to disclose cybersecurity incidents. In line with this principle, companies listed on US stock exchanges are obliged to disclose any material cybersecurity incidents within a certain period. This requirement is based on an investor protection justification under the theory of agency. It aims at minimizing the informational disparity between the companies and the investors. Another element of the model is the requirement to disclose cybersecurity governance issues, including board oversight, expertise of the company's management in cybersecurity issues, and risk management. The rule also covers strategy and risk management disclosure. Thus, the company is expected to present the methods used to identify, assess, and mitigate cybersecurity risks.

It is possible to highlight several strengths of the model. First, the main idea behind the proposed regulation is to foster transparency. Second, the SEC's framework will contribute to improved information efficiency of capital markets and help investors better understand the risk involved in investing in a particular company. Recent empirical research supports this view and suggests that cybersecurity disclosures affect investor behavior, firm valuation, and insider trading (Huang & Murthy, 2024; Chen et al., 2025).

However, the model under consideration faces some disadvantages. First, while increasing transparency about cybersecurity incidents, the disclosure-based framework does not guarantee the implementation of adequate cybersecurity measures by the companies. Second, disclosure is an ex-post mechanism that cannot prevent the risks from emerging. Third, the focus on issuer-level reporting means that the intermediary networks through which cybersecurity risks can propagate are ignored. Therefore, the SEC's model is effective in fostering transparency but insufficient in managing cybersecurity risks in digital capital markets.

European Union: Resilience-Led Response

Unlike the U.S., however, the European Union has adopted an approach that puts a strong emphasis on resilience, introducing the new regulatory instrument called the Digital Operational Resilience Act (DORA). The DORA regulatory regime implies the development of a holistic regulatory scheme for managing various types of ICT-related risks in the finance sector. Hence, the shift from disclosure-oriented regulation towards a more operational approach and systems thinking can be traced (Buttigieg & Brunelli Zimmermann, 2024).

The DORA regulatory framework includes a wide range of prerequisites such as ICT risk management, ICT-related incident reporting, resilience testing, and third-party supervision. Financial entities will be required to develop strong internal controls, conduct resilience tests that include both penetration testing and scenario analysis, and establish an effective incident response/recovery plan. In addition, DORA includes provisions for direct supervision of critical ICT providers.

It should be noted that, unlike many other regulatory regimes, the DORA framework applies to the entire financial sector without any exemptions. In this sense, the EU approach can be characterized as holistic and taking into account all the elements involved in a cyber-governance environment and the need for systemic resilience in the financial sector.

From the standpoint of architectural integrity and operational capabilities, the DORA regime seems to be one of the most advanced solutions for the time being due to the integration of a wide range of factors, such as governance, risk management, testing, and third-party oversight into one single system, thus ensuring systems-level thinking as well.

At the same time, such a framework can pose certain problems in terms of compliance. First of all, given its complexity, DORA will pose a heavy burden on small institutions; in particular, compliance might be difficult to achieve in terms of infrastructure. Another aspect that should not be underestimated is the potential lack of supervisory coordination between various European authorities. As shown in the literature, the success of any comprehensive system requires effective monitoring (Buttigieg & Brunelli Zimmermann, 2024).

IOSCO / CPMI-IOSCO: Market-Wide Resilience Logic

At the international level, cybersecurity regulations are influenced by various principles and guidance documents issued by standard-setters like the International Organization of Securities Commissions (IOSCO)

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

and Committee on Payments and Market Infrastructures (CPMI), working in conjunction with IOSCO. The frameworks have a market-wide resilience approach in which the cyber risk is viewed as a threat to market integrity, financial stability, and continuity of critical financial operations.

According to IOSCO's guidelines for market outages and cyber risk, operational resilience should be fostered in markets to maintain orderly conditions in times of technical disruptions and cyberattacks (IOSCO, 2024). CPMI-IOSCO's guidance for cyber resilience in financial market infrastructures (FMIs) focuses on the ability of FMIs to detect, withstand, respond to, and recover from attacks. Financial market infrastructures (FMI) are critical for financial operations and therefore require special attention from the regulator.

A characteristic feature of the frameworks is the focus on systemic aspects and interconnectivities, especially in FMIs (exchanges, central counterparties, and settlement systems). It means that the disruption of such systems could trigger cascading effects across the financial system. That is why, according to the frameworks, the issue requires coordinated responses, information exchange, and international cooperation.

The strengths of the IOSCO and CPMI-IOSCO frameworks are related to their systemic nature and international applicability. Offering general high-level standards and guidance documents, the organizations help harmonize and converge efforts at the global level and ensure resilience and interoperability of financial systems. The frameworks address the issue of market-wide stability alongside the national regulations and compensate for the fragmentation of jurisdiction.

However, the frameworks' nonbinding nature can be seen as one of their weaknesses since implementation is voluntary and dependent on the national authorities. Hence, some variations might arise due to different approaches to regulation, and certain jurisdictions may be less prepared than others regarding resilience and cyber threats, potentially creating vulnerabilities at the global level. Nevertheless, the IOSCO and CPMI-IOSCO frameworks play an important role in regulating cybersecurity risks on an international level.

Comparative analysis reveals the existence of three main directions of the regulation of the cyber risk, namely disclosure, resilience, and systemic coordination. The U.S. model places the focus on disclosure and investors' rights and interests. The EU approach emphasizes the importance of operational resilience and coherence, while international standards deal mainly with systemic and cross-border issues. Although each of the frameworks addresses the relevant issues, no single approach is comprehensive.

In order to effectively manage cybersecurity risks in digitized capital markets, an integrative model combining all the mentioned features should be developed and adopted. Comparative table illustrating the regulatory regimes' structural differences, content, and other important characteristics is shown below (see Figure 3).

Regulatory Dimensions	United States	European Union	Singapore	Japan
Disclosure Requirements	SEC Cyber Disclosure Rules	NFRD / CSRD	MAS Disclosure Guidelines	FSA Cyber Disclosure Rules
Operational Resilience	NIST Cyber Framework	DORA	Cyber Hygiene Notices	FISC Security Guidelines
Third-Party Risk Management	OCC Third-Party Guidance	EU Outsourcing Guidelines	MAS Outsourcing Rules	FSA Vendor Risk Rules
Incident Reporting	CISA Reporting Mandates	NIS Directive	MAS Incident Reporting	FSA Incident Rules
Penalties & Enforcement	SEC & FINRA Sanctions	GDPR Fines	MAS Enforcement Actions	FSA Administrative Sanctions
Regulatory Guidance	FFIEC Cyber Guidance	ESMA & EBA Guidelines	MAS Technology Guidelines	JFSA Cyber Guidance

Figure 3: Comparative Regulatory Framework Matrix for Cybersecurity in Capital Markets.

This figure presents a structured comparison of cybersecurity regulatory approaches across major jurisdictions, highlighting differences in disclosure requirements, operational resilience, third-party risk management, incident reporting, enforcement mechanisms, and regulatory guidance. It illustrates the divergence and partial convergence of regulatory models, emphasizing the contrast between disclosure-driven, resilience-oriented, and hybrid governance frameworks.

Source: Author's compilation based on Buttigieg and Brunelli Zimmermann (2024), Huang and Murthy (2024), Gao and Calderon (2025), Kotidis and Schreft (2025), U.S. Securities and Exchange Commission (2023), and International Organization of Securities Commissions (2024).

DISCUSSION AND POLICY IMPLICATIONS

As shown in the current research, there is an emerging trend whereby the response of regulation to cybersecurity risks in capital markets digitized through new technologies seems to be experiencing an interesting transformation whereby a convergence to a more comprehensive approach to governance of cyber risks appears to be slowly happening, although not fully. In the past, cybersecurity risks were largely perceived as being purely technical in nature and dealt with at the individual company's level. This trend has since changed, according to the evolving understanding of the nature of cybersecurity, which now sees it as an issue of market governance.

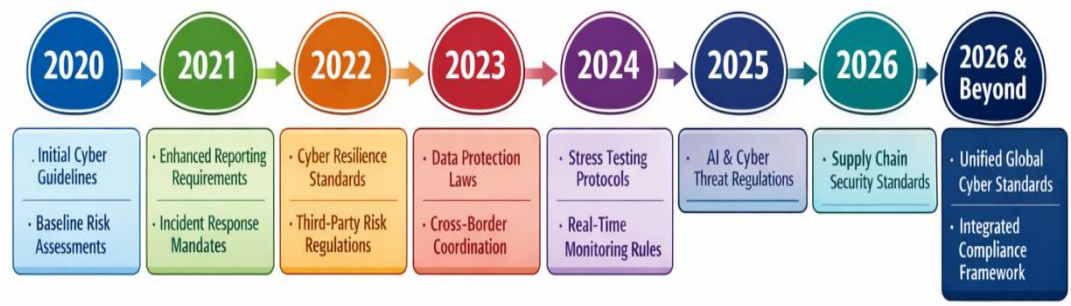

Figure 4: Regulatory Evolution Timeline of Cybersecurity Governance in Capital Markets (2020–2026).

This figure illustrates the progression of cybersecurity regulatory frameworks in capital markets from 2020 to 2026, highlighting the transition from fragmented, compliance-based approaches toward integrated models emphasizing disclosure, operational resilience, third-party risk governance, and systemic coordination. It captures key milestones in regulatory development, including enhanced reporting requirements, resilience standards, cross-border coordination, and the emergence of global cyber governance frameworks.

Source: Author's conceptualization based on Buttigieg and Brunelli Zimmermann (2024), International Organization of Securities Commissions (2024, 2025), U.S. Securities and Exchange Commission (2023), Huang and Murthy (2024), and Gao and Calderon (2025).

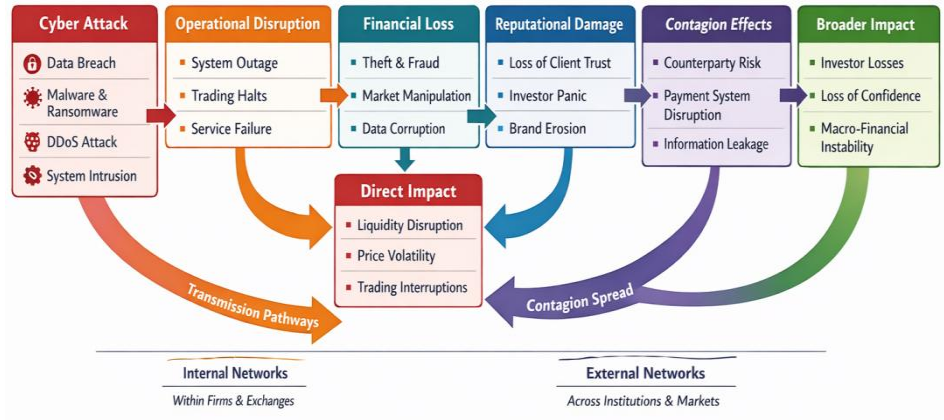

Figure 5: Cyber Risk Transmission and Contagion Pathways in Capital Markets.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

This figure illustrates the sequential and interconnected pathways through which cybersecurity incidents propagate across capital markets, from initial cyberattacks to operational disruptions, financial losses, reputational damage, and systemic contagion effects. It highlights how cyber risks spread through internal networks within firms and external interconnections across institutions, ultimately leading to broader market instability, liquidity disruptions, and loss of investor confidence.

Source: Author's conceptualization based on Kotidis and Schreft (2025), International Organization of Securities Commissions (2024), Zhang and Wong (2025), and Tan et al. (2025).

The main insight that follows from the analysis above is that modern regulatory regimes increasingly incorporate aspects of both disclosure-oriented and resilience-oriented frameworks, but remain highly fragmented institutionally and conceptually. Disclosure-focused regulatory regimes, characteristic of jurisdictions like the US, place an emphasis on transparency and the provision of information for investors and regulators alike in line with agency theory concerns around information asymmetry. There is robust empirical evidence supporting the validity of the approach, which shows that cybersecurity disclosures indeed impact how investors make decisions and assess company value (as well as engage in insider trading activities) (Huang & Murthy, 2024; Chen et al., 2025). Meanwhile, resilience-focused frameworks in the EU recognize the broader implications of cyber risk as an operational risk and a systemwide phenomenon that requires management.

Nonetheless, the fact that both disclosure-oriented and resilience-oriented regulatory regimes exist simultaneously fails to imply the integration between them. The first gap identified concerns fragmentation between the two types of regimes, whereby a focus on disclosure may increase transparency but not lead to resilience. At the same time, resilience-oriented regimes might include strong internal control mechanisms and testing requirements, but fail to incorporate adequate mechanisms for disclosure of information relevant for investors. Hence, there are important philosophical and structural differences between the two categories of regimes that result in inconsistencies in how cybersecurity risks can be addressed by regulators.

A second potential gap in existing frameworks concerns the insufficient treatment of risks posed by the third party dependency and concentration issues. Modern capital markets rely increasingly on ICT services provided by third parties, most notably cloud platform providers, which means that cyber risk is no longer contained within individual companies but affects the entire ICT-dependent ecosystem. While the DORA framework explicitly deals with risks related to the outsourcing of ICT services, other disclosure-based regimes fail to take into account how third-party risks are managed. Evidence shows that cyber-related disruptions can indeed spread through the ICT infrastructure of service providers and have negative effects on systemic resilience (Kotidis & Schreft, 2025). Consequently, third-party risks are a critical aspect of cyber risk that needs better regulatory oversight.

A third possible gap is related to the uneven attention paid to the systemic consequences of cyber incidents in terms of market outages, loss of liquidity, and propagation. Whereas the International Organization of Securities Commissions and Committee on Payments and Market Infrastructures – IOSCO emphasize the need to build resilience in financial market infrastructures, national-level regulatory frameworks tend to overlook these considerations, focusing instead on disclosure or sectoral risk management issues. The existing research suggests that cyber risks can indeed impact liquidity in stock markets, causing adverse consequences for investors' decisions and market efficiency (Zhang & Wong, 2025; Tan et al., 2025).

Collectively, these findings reveal that regulatory regimes for cyber risks in capital markets are indeed evolving positively, but have not yet converged sufficiently to achieve adequate regulatory oversight. On the one hand, the current state of affairs is characterized by partial convergence of three types of considerations: disclosure-related, resilience-related, and systemic considerations. On the other hand, inconsistencies in the approaches taken by various jurisdictions prevent the development of a truly effective system of cybersecurity governance.

In light of the gaps identified, multiple policy implications can be considered. First, there is a need to elaborate a multi-layered cyber regulation framework in capital markets that takes into account differences in roles

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

played by market actors. The suggested framework will distinguish among regulatory requirements placed upon issuers (who primarily need to disclose information), market intermediaries (who are responsible for managing risks associated with their business), and financial market infrastructures (whose primary objective should be to maintain resilience and continuity).

Second, existing regulatory regimes in various jurisdictions could benefit from the harmonization of definitions used (such as "material cybersecurity incident" or "major ICT incident") as well as reporting frameworks. This will allow for consistent application of the regimes and facilitate cross-border supervision.

Third, it is crucial to develop adequate supervisory approaches to third-party service providers in light of their criticality to the functioning of capital markets. Specifically, it would be important to identify third parties whose operations are critical and then develop supervisory powers in relation to them.

Fourth, regulatory regimes should integrate the issue of market outages, which is especially relevant in the context of cybersecurity risks. Market outage preparedness and the development of coordinated strategies for responding to them will significantly enhance systemic resilience of financial systems.

Fifth, there is a need to standardize cybersecurity disclosures by developing adequate frameworks. While information about cyber risks should be available to investors, certain information might be sensitive and cause security issues. Hence, regulatory frameworks should clearly define the scope of required disclosures.

In conclusion, cyber regulation in capital markets is shifting from sector-specific cybersecurity to a broader cybersecurity governance framework. To be effective, such frameworks require more sophisticated, coordinated, and integrated approaches that address specific gaps identified herein.

CONCLUSION

This study explores the question of adequacy of present-day regulatory frameworks in terms of mitigating cybersecurity risks emerging in the context of digitization of capital markets. Findings presented below clearly show that while current regulatory approaches have become more sophisticated and sensitive to the changing reality of cybersecurity challenges, they lack structural integrity and integration on both national and international levels.

There are numerous indications that the process of integrating cybersecurity into the general regulatory framework governing the functioning of capital markets and securities industry in various countries has progressed significantly. While initially cybersecurity was regarded simply as a technical aspect of the problem, now this dimension has been firmly incorporated into wider regulatory and governance processes related to the areas of market operations and financial stability, as well as investor protection.

However, despite obvious progress observed at the national and global level, the existing model does not represent a coherent framework in terms of its coverage of cybersecurity issues related to capital markets. The available approaches represent partially converged regulatory logics of disclosure, resilience, and systemic oversight aimed at solving only particular aspects of the challenge in question. Disclose regimes promote greater transparency and facilitate the processes of making decisions on investments, according to research findings (Huang & Murthy, 2024; Gao & Calderon, 2025). In turn, resilience-focused regimes provide for improved internal controls and regular testing and recovery measures, thus indicating greater proactivity from the regulatory bodies (Buttigieg & Brunelli Zimmermann, 2024). International frameworks highlight the systemic dimensions of cyber risks for capital markets and financial market infrastructures, focusing on the consequences of disruptions at the market-wide level (IOSCO, 2024).

Nonetheless, despite all these achievements, the area of cybersecurity regulations related to capital markets still suffers from lack of coherence and integration of different approaches. There still exists a fragmentation between disclose and resilience-based approaches, thereby limiting the effectiveness of regulatory intervention. Third-party dependency and concentration risks are addressed unsatisfactorily, even though they became ever more important with the advent of digital interconnectedness of modern capital markets. Furthermore, market-

wide systemic dimensions of cyber risks are given little thought at the expense of narrower perspectives of disclosure and operational resilience (Kotidis & Schreft, 2025; Zhang & Wong, 2025).

Therefore, the present study concludes that for a successful solution to the existing challenges it will be necessary to develop a new model of capital markets cyber regulation combining investor-centric transparency, corporate resilience, and market systemic dimension. To implement such an approach in practice, there is a need for harmonization of definitions and regulatory standards as well as coordinated actions of national and international regulatory authorities.

REFERENCES

1. Amani, F., Magnan, M., & Moldovan, R. (2025). Cybersecurity risks and incidents disclosure: A literature review. Accounting Perspectives, 24(3), 605–667. https://doi.org/10.1111/1911-3838.12411
2. Buttigieg, C. P., & Brunelli Zimmermann, B. (2024). The digital operational resilience act: Challenges and reflections on the adequacy of Europe's supervisory architecture. ERA Forum, 25, 11–28. https://doi.org/10.1007/s12027-024-00793-w
3. Chen, X., Hilary, G., & Tian, X. (2025). Mandatory data breach disclosure and insider trading. Journal of Business Finance & Accounting, 52(5–6), 2091–2110. https://doi.org/10.1111/jbfa.12842
4. European Insurance and Occupational Pensions Authority. (2026). Digital operational resilience act (DORA). https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
5. European Securities and Markets Authority. (2026). Digital operational resilience act (DORA). https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora
6. 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. Official Journal of the European Union, L 333, 1–79. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
7. Gao, L., & Calderon, T. G. (2025). Cybersecurity risk governance and corporate cybersecurity risk disclosures. Journal of Accounting and Public Policy, 54, 107376. https://doi.org/10.1016/j.jaccpubpol.2025.107376
8. Huang, J., & Murthy, U. (2024). The impact of cybersecurity risk management strategy disclosure on investors' judgments and decisions. International Journal of Accounting Information Systems, 54, 100696. https://doi.org/10.1016/j.accinf.2024.100696
9. International Organization of Securities Commissions. (2024). Market outages (Final Report No. FR04/2024). https://www.iosco.org/library/pubdocs/pdf/IOSCOPD767.pdf
10. International Organization of Securities Commissions. (2025). Annual report 2024. https://www.iosco.org/annual_reports/2024/pdf/annualReport2024.pdf
11. Kotidis, A., & Schreft, S. L. (2025). The propagation of cyberattacks through the financial system. The Journal of Finance, 80(6), 3313–3358.
12. Tan, W., Guo, B., & Zhang, Q. (2025). Cybersecurity governance and corporate market value: Perspectives from investor trust and supply chain trust. Pacific-Basin Finance Journal, 90, 102646. https://doi.org/10.1016/j.pacfin.2024.102646
13. U.S. Securities and Exchange Commission. (2023a). Cybersecurity risk management, strategy, governance, and incident disclosure (Release No. 33-11216). https://www.sec.gov/files/rules/final/2023/33-11216.pdf
14. U.S. Securities and Exchange Commission. (2023b, July 26). SEC adopts rules on cybersecurity risk management, strategy, governance, and incident disclosure. https://www.sec.gov/newsroom/press-releases/2023-139
15. Zhang, Q., & Wong, J. B. (2025). Cybersecurity risks and stock liquidity. International Journal of Managerial Finance, 21(3), 841–861. https://doi.org/10.1108/IJMF-05-2024-0253