Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 05| Issue- 04| 2026

Research Article **Received:** 10-03-2026 | **Accepted:** 05-04-2026 | **Published:** 19-04-2026

Technology-Driven Risk Governance in U.S. Financial Reporting: The Role of Cybersecurity Disclosure and Regulatory Technology in Strengthening Capital Market Transparency

***Kingsford Brakye*[1] *and Mary Magdalene Yeboah*[2]**

[1]*Dakota State University, USA*

[2]*University of Ghana Business School, Ghana*

Abstract: The rapid digitalization of the financial reporting systems has exposed the U.S. public companies to cybersecurity threats that could impair financial information integrity, the reliability of disclosure, and investor confidence. This paper examines how cybersecurity risk disclosure practices and regulatory technology adoption affect transparency and accountability in US capital markets. The study reviewed existing literature, regulatory guidance, and corporate disclosures in the filings of U.S. public companies, 2020-2026, using a qualitative analytical approach. The results show that the disclosure of cyber risk in corporate reporting is becoming visible in recent years, with the advent of new laws, such as new mandatory cybersecurity disclosure regulations through Regulation S-K. It is also indicated that cybersecurity incidents continue to affect investor perceptions, though the market reactions to breach announcements have been declining over time. Continuous internal control risks are also a major issue to the reliability of the reporting, and the use of Regulatory Technology tools has enhanced monitoring, compliance procedures, and accuracy in reporting. Nevertheless, the growing reliance on automated compliance mechanisms also presents a governance issue to boards and audit committees, charged with the responsibility of monitoring the complex technology-based reporting systems.

Keywords: Cybersecurity Disclosure, Regulatory Technology, Internal Controls, Capital Market Transparency, Risk Governance.

INTRODUCTION

The growing level of digitization of corporate activities has significantly altered financial reporting in the U.S. capital markets (Velte, 2023). With increasing dependency on a digital infrastructure and built-in information systems by firms, cybersecurity risks have become a material risk that can impact financial data integrity, operational continuity, and investor confidence (Tosun, 2021; Issayeva *et al*., 2023). Cybersecurity attacks have the potential to interfere with financial reporting, reveal confidential data, and introduce uncertainties within the capital markets (Bederna & Szádeczky, 2023). Consequently, cybersecurity risk management and disclosure are now regarded as vital aspects of corporate governance by investors, regulators, and corporate boards (Brakye & Adam, 2025).

To address these issues, the regulatory entities in the United States have enhanced the expectations regarding cybersecurity risk reporting and governance (U.S. Securities and Exchange Commission, 2023). Disclosure requirements under the Securities and Exchange Commission's Regulation S-K, including Item 106 and Item 1.05, require public companies to provide more structured information about cybersecurity risk management practices and material cyber incidents (U.S. Securities and Exchange Commission, 2023). These advancements are indicative of an overall regulatory initiative to enhance transparency and provide investors with sufficient and timely information regarding technology-related risks that can impact the value of firms (Financial Stability Oversight Council, 2025).

Simultaneously, to cope with the complicated compliance requirements and enhance the process of internal controls, organizations gradually adopt Regulatory Technology (RegTech) solutions (Jeyasingh, 2023). These technologies support automated monitoring, risk detection, and reporting functions that help firms respond more efficiently to regulatory expectations and operational risks (Azubuike, 2024). Nevertheless, even with the increasing regulatory focus and technological advancement, key questions exist on the interaction between cybersecurity disclosure, internal control effectiveness, and technologically enabled compliance systems in financial reporting settings (Elsayed & Elshandidy, 2021).

Although increasing attention is being paid to cybersecurity disclosure, internal control governance, and regulatory technology adoption, most of the current studies cover them separately (Charoen & Khern-am-nuai, 2025). Research on cybersecurity disclosure is usually centered on market responses to data breaches, and research on internal control systems is mainly on the quality of financial reporting and audit results (Cao *et al*., 2024). In the same manner, studies of regulatory

***Corresponding Author:** Kingsford Brakye

DOI- https://doi.org/10.5281/zenodo.19654718

technology are inclined towards automating compliance and monitoring efficiency (Jeyasingh, 2023). Nevertheless, few studies have investigated the interplay of these factors in financial reporting systems and the overall impact of their aggregate effect on transparency in the U.S. capital markets (Velte, 2023). This gap makes it difficult to fully understand the governance mechanisms that support reliable financial reporting in an increasingly digital environment.

This study is relevant to the existing body of literature on financial reporting governance because it focuses on the relationship between cybersecurity disclosure practices, internal control effectiveness, and regulatory technology adoption among U.S. public firms (Elsayed & Elshandidy, 2021). Through the combination of these aspects of governance, the research would offer a wider perspective of how technology-based risk management affects transparency and reliability in financial reporting systems (Jeyasingh, 2023). The results also provide ideas on how companies can enhance digital risk management and enrich disclosure practices following the changing regulatory demands in the United States (Brakye & Adam, 2025).

This study discusses technology-based risk governance in the U.S. financial reporting systems between 2020 and 2026. Precisely, it examines the role of cybersecurity risk disclosure practices, internal control weaknesses, and the adoption of regulatory technology in driving transparency in capital markets. The main research question that will inform this study is how the practices of cybersecurity risk disclosure in financial reporting can contribute to strengthening transparency and accountability in the U.S. capital markets. This study contributes to the literature in three ways. First, it integrates cybersecurity risk disclosure, internal control governance, and regulatory technology adoption within a unified technology-driven risk governance framework. Second, it synthesizes recent empirical and regulatory developments between 2020 and 2025 to explain how cybersecurity reporting practices influence capital market transparency. Third, the study provides governance and regulatory implications for corporate boards, auditors, and policymakers navigating technology-driven financial reporting environments. The study, through the analysis of these interdependent governance mechanisms, helps to understand more effectively how firms can enhance the credibility of their financial reporting and keep investors confident in a more digital financial world.

LITERATURE REVIEW

Current literature has materially explored the financial and governance consequences of cybersecurity risks within corporate reporting environments (Issayeva *et al*., 2023; Tosun, 2021). Preliminary literature was dedicated to investigating the implications of cybersecurity breaches on the market, and in particular, how investors react to publicly disclosed cyber incidents (Tosun, 2021). Recent studies indicate a tendency toward the weakening of market responses to breach announcements. Indicatively, Charoen *et al*. (2024) note that the adverse market reaction to breach disclosures between 2013 and 2021 has weakened in relation to prior years, indicating that investors might have become accustomed to cyber risk disclosures. However, certain events may still have quantifiable market effects. There is evidence that first-time hacks may result in a decrease in firm value, such as an average decrease of about 88 basis points in daily excess returns following the announcement of a breach (Issayeva *et al*., 2023).

Studies also indicate that corporate disclosure practices have been changing in an effort by companies to cope with investor responses to cybersecurity attacks (Brakye & Adam, 2025). Firms are increasingly relying on elaborate written reports on disclosures on cyber risks and remediation activities, especially after the regulatory guidelines that promote more transparency in risk reporting (U.S. Securities and Exchange Commission, 2023). Simultaneously, variance between firms is high. Smaller firms are also more likely to suffer adverse market impacts of breach announcements than larger firms, which usually have better governance procedures and resources to effectively address cyber risks (Issayeva *et al*., 2023). Research also indicates that the complexity of financial reporting may be heightened following a cyber incident, especially in XBRL filings, where companies may include more explanatory narratives in financial statement notes to minimize market uncertainty (Jiang *et al*., 2024).

Besides disclosure practices, internal control systems are also very important in deciding on the reliability of financial reporting (Elsayed & Elshandidy, 2021). According to earlier literature, the presence of persistent material weaknesses in internal controls is a significant challenge to the

Publisher: SARC Publisher

quality of financial reporting (Tian *et al*., 2025). Empirical results show that about one-third of material weakness disclosures remain for more than several years, and that firms have reported similar weaknesses over a period of more than 10 years (Tian *et al*., 2025). These ongoing control failures are related to increased audit fees, longer reporting delays, and increased probability of financial misstatements (Fischer *et al*., 2020). Some studies also indicate that companies with better internal control mechanisms are more likely to make more informative disclosure of risks, and this can enhance market liquidity and reduce asymmetry of information (Elsayed & Elshandidy, 2021). Nevertheless, there are still governance issues. To illustrate, audit committee oversight research suggests that too much oversight responsibility can result in what is commonly defined as the audit committee overload, which can adversely impact financial reporting quality and increase the risk of financial restatements (Ashraf *et al*., 2024).

The regulatory environment of cybersecurity disclosure has also been influenced by the recent developments in policies (U.S. Securities and Exchange Commission, 2023). Alterations in enforcing priorities in the U.S. Securities and Exchange Commission have shifted the corporate cyber governance landscape (Fischman *et al*., 2026). By 2025, enforcement activity had reduced considerably, with the Commission moving to a more focused enforcement approach of direct investor harm cases (Fischman *et al*., 2026). Meanwhile, the SEC reorganized its enforcement framework by establishing a Cyber and Emerging Technologies Unit to deal with the risk posed by cybersecurity and digital innovation (U.S. Securities and Exchange Commission, 2023). Among the most notable breakthroughs of the cybersecurity governance was the settlement of the SolarWinds litigation over claims of false cybersecurity reporting (Fischman *et al*., 2026). The case showed how corporate officers involved in cybersecurity management could be held liable and the significance of making correct statements publicly about cyber risk management behaviors. Consequently, many organizations have enhanced internal audit processes of cybersecurity disclosures and enhanced liaisons between technical security departments and corporate reporting units.

The legal standards applied in the enforcement actions in cybersecurity have also been affected by the regulatory developments. Recent enforcement trends are showing a trend towards the scienter-based theories of fraud requiring proof of intentional or reckless misconduct as opposed to mere negligence (Fischman *et al*., 2026). This modification can lead to less regulatory uncertainty among the firms that engage in good-faith disclosure efforts and enhanced investigation of the cases of intentional concealment of cybersecurity risks. Although there is an increasing body of research on cybersecurity disclosure, internal control governance, and adoption of regulatory technology, the available literature has mainly analyzed these matters independently of one another (Jeyasingh, 2023). Although research has examined the market responses to cyber incidents and the governance consequences of internal control weaknesses, there is a dearth of research investigating the interactions between cybersecurity disclosure practices and internal control systems and technology-based compliance-supporting tools in financial reporting contexts. With the continued development of digital financial systems, how all of these governance mechanisms affect the overall transparency of financial reporting is another topic of interest that needs to be studied further.

Conceptual Framework

In this study, a technology-based risk governance framework will be used to articulate the role of cybersecurity risk disclosure in financial reporting in enhancing transparency and accountability in U.S. capital markets. With the growing reliance of firms on digital systems to facilitate the financial reporting process, the issue of cybersecurity risks has emerged as a critical aspect that influences the credibility of the financial information and the trust of the market participants (Issayeva *et al*., 2023; Tosun, 2021). In the event of cybersecurity incidents, organizations need to consider the possible effects on operations, financial reporting, and investor information (Bederna & Szádeczky, 2023). The way these risks are reported thus is significant in determining the way investors and regulators evaluate the governance and reporting quality of a firm (Brakye & Adam, 2025). Cybersecurity risk disclosure is the main tool in this framework by which firms disclose to the capital market their digital risk exposure. The disclosure of cyber incidents, risk management practices, and the structure of governance enables investors to have a better assessment of the stability of the operations of a firm as well as the financial implications of cyber threats. The reporting of these risks transparently can help in

Publisher: SARC Publisher

minimizing information asymmetry between corporate managers and investors, which will enhance confidence in the market and accountability of corporate reporting practices (Elsayed & Elshandidy, 2021).

Nevertheless, the efficiency of cybersecurity disclosure is subject to the internal control environment in the organization. Internal controls over financial reporting impact the manner in which cyber incidents are identified, assessed, and reported in the financial disclosures (Elsayed & Elshandidy, 2021). Companies that have more robust control mechanisms have a better chance of detecting cybersecurity risks promptly and conveying the appropriate information correctly in regulatory disclosures. On the other hand, recurring internal control failures can make cybersecurity reporting less credible and create a state of uncertainty, especially among investors (Tian *et al*., 2025). The framework also takes into account the role of regulatory technology (RegTech) as a governance supporting mechanism. Financial institutions and public companies have started adopting Regulatory Technology tools to track regulatory demands, streamline regulatory compliance procedures, and keep proper records of reporting. These technologies can be used to improve the consistency and timeliness of cybersecurity disclosures in financial reporting systems by improving monitoring and documentation processes (Azubuike, 2024). Collectively, the framework suggests that cybersecurity risk disclosure practices affect capital market transparency because of the interaction with internal control systems and technology-enabled compliance mechanisms. Firms that integrate transparent disclosure practices with quality internal controls and effective monitoring tools are better positioned to offer credible financial information to the investors and regulators. This connection is the foundation of examining the role of cybersecurity disclosure in strengthening the transparency and accountability in U.S. capital markets.

METHODOLOGY

The qualitative analytical approach in this study uses secondary sources of data to analyze the impact of cybersecurity risk disclosure practices in financial reporting on the transparency and accountability of the U.S. capital markets. Instead of gathering direct survey or interview data, the analysis will be based on publicly available regulatory filings, scholarly research, and empirical studies reporting on cybersecurity disclosure practices and their impact on financial reporting results. This method is suitable since the practices of cybersecurity reporting and the market response have already been extensively studied based on archival financial records and regulatory disclosures. The main sources of information utilized in this research are scholarly articles published within the period of 2020-2026, publicly traded companies that have submitted corporate filings to the Securities and Exchange Commission, and empirical research through recognized financial databases, including Audit Analytics, CRSP, and Compustat. A total of 22 peer-reviewed articles, regulatory reports, and empirical studies were reviewed and synthesized in this study. Previous studies with these data sets have provided an analysis of market responses to announcements of cybersecurity breaches, internal control deficiencies, and the disclosure of corporate filings. This study analyzes the relationship between cybersecurity disclosure practices and financial reporting governance systems and determines its impact on capital market transparency by synthesizing the results of these studies. Moreover, the research takes into account cybersecurity disclosures in the Item 1C sections of the 10-K filings with financial regulators and policies reports of financial oversight entities like the Financial Stability Oversight Council (FSOC) to offer a wider regulatory framework in the area of cybersecurity governance and financial reporting transparency.

Besides empirical research, regulatory guidance and disclosure requirements that impact cybersecurity reporting are taken into account in the analysis. The filings of the public companies (Form 10-K and Form 8-K) are evidence of how companies report on cybersecurity threats, cybersecurity incident responses, and governance mechanisms to investors. Special consideration is given to such disclosures as those associated with cybersecurity incidents that are reported in accordance with Regulation S-K reporting requirements. Such filings enable an understanding of how companies define material cyber risks and incorporate them in their financial reporting systems.

The methodology of this research is the examination of empirical evidence concerning three related topics: the disclosure of cybersecurity breaches and the investor response, internal control effectiveness in financial reporting, and the role of compliance technologies in facilitating corporate

Publisher: SARC Publisher

governance. Comparing the outcomes of these research streams, the research establishes patterns in the effectiveness of cybersecurity disclosure practices in affecting financial reporting transparency and investor information. The synthesis will enable the study to determine whether improvements in disclosure practices, governance oversight, and monitoring technologies contribute to enhancing accountability in capital markets. On the whole, this approach involves regulatory disclosure analysis along with the archival financial research results to assess the connection between cybersecurity risk reporting and transparency in the U.S. financial markets. In this manner, this study relies on verifiable evidence from financial databases, regulatory filings, and peer-reviewed research to demonstrate how cybersecurity disclosure practices influence the reliability and credibility of financial reporting in a growing digital corporate context.

RESULTS AND FINDINGS

The subsequent results review tendencies in cybersecurity disclosure practices and their impact on financial reporting transparency in the U.S. capital markets. The findings are interpreted through the technology-driven risk governance framework developed in this study, highlighting how cybersecurity disclosure practices, internal control effectiveness, and regulatory technology adoption collectively influence financial reporting transparency.

Trends in Cybersecurity Disclosure and Market Reaction to Cybersecurity Breaches

Recent regulatory changes have affected the disclosure of cybersecurity incidents in financial reporting by firms. There is some evidence that disclosures of cybersecurity breaches reported in 2025 under Item 1.05 of Form 8-K have decreased significantly, with only seven disclosures of cybersecurity breaches reported between January and July 2025 as compared with nineteen disclosures of cybersecurity breaches reported between January and July 2024. This constitutes a decrease in reported incidents by about 63 percent.

This change can be attributed to several factors. Regulatory guidance made it clear that only material cybersecurity incidents should be reported, which minimized the chances that companies would report all cyber incidents (U.S. Securities and Exchange Commission, 2023). Moreover, the legal departments of companies have been more conservative with their materiality determinations after high-profile enforcement cases involving cybersecurity disclosures (Fischman *et al*., 2026). Corporate incident response program improvements can also contribute to it, with companies becoming more effective in identifying and containing cyber incidents before they escalate to the stage where they have to be reported to the public. According to these developments, cybersecurity reporting is slowly transitioning to more structured and selective disclosure practices. As cyber incidents continue to be widespread across the world, the standard of reporting them in financial reports seems to be progressively pegged to material financial impact.

Previous studies demonstrate that cybersecurity events are capable of affecting the valuation of a firm and the perception of investors (Issayeva *et al*., 2023; Tosun, 2021). Empirical evidence also shows that the first instance of hacking is linked to quantifiable market responses, such as an average 88 basis point decline in the daily excess returns following the announcement of breaches (Issayeva *et al*., 2023). At the same time, recent studies suggest that investor reactions to cybersecurity disclosures have weakened over time. With cyber incidents becoming more frequent and with disclosure practices becoming more standardized, investors are likely to view cybersecurity risk as an operational risk more often than a shock. This phenomenon has been described in the literature as the "disappearing cost" of data breach disclosures (Charoen & Khern-am-nuai, 2025).

However, not all cyber incidents produce the same market response. The incidences of breaches of sensitive customer data or major disruptions in operations still produce greater negative responses. The quality of corporate disclosure is important as well. Firms that disclose cyber incidents and recovery measures in detail tend to have more moderate responses in the market as opposed to companies that make disclosures that are vague or delayed (Brakye & Adam, 2025).

Firm Size and Disclosure Outcomes

Firm size plays an important role in how cybersecurity incidents affect financial markets (Issayeva *et al*., 2023). Big firms tend to have more resources to handle cybersecurity risks and communicate those effectively to investors. This means that market responses to cyber attacks are less severe for large companies, which are usually viewed as being more financially endowed and well-organized to internalize the expenses of cyber

Publisher: SARC Publisher

attacks (Bederna & Szádeczky, 2023). Smaller firms face greater challenges in this area.

They also usually lack the means to invest in the development of such advanced cybersecurity systems and compliance monitoring tools. As a result, smaller organizations have a greater probability of facing more severe negative market responses in the event of cybersecurity incidents (Issayeva *et al*., 2023). They also incur relatively higher costs in adopting technologies that aim at enhancing monitoring, disclosure, and regulatory compliance. These differences imply that the capabilities of cybersecurity governance can change the manner in which markets process disclosure events. Firms that have a more robust system of governance can be in a better position to retain investor confidence in the event of a cybersecurity incident (Brakye & Adam, 2025).

Internal Control Weakness and Financial Reporting Transparency

Internal control effectiveness is a key factor in the credibility of financial reporting disclosures (Elsayed & Elshandidy, 2021). Persistent material weaknesses in internal control over financial reporting remain a major concern in corporate governance research (Tian *et al*., 2025). The evidence demonstrates that about one-third of disclosed material weaknesses continue to exist over several years, and in other cases, the same weakness continues over a period of over 10 years. Persistent internal control deficiencies are associated with several negative reporting outcomes. Firms whose weaknesses are recurrent are mostly charged with greater audit fees and reporting delays, as auditors have to carry out extra audit procedures to ensure that the financial information is reliable (Fischer *et al*., 2020). In some cases, audit fees may increase by as much as 65 to 99 percent during extended periods of internal control weakness (Fischer *et al*., 2020). The quality of disclosure is also influenced by the effectiveness of internal controls. Strong informative risk disclosures are given by firms that have stronger control systems, and this can eliminate information asymmetry between firms and investors (Elsayed & Elshandidy, 2021). Conversely, the continuous poor performance enhances the chances of financial misstatements and low confidence in corporate reporting practices (Velte, 2023).

The role of Regulatory Technology in Compliance and Reporting

The growing use of regulatory technology has introduced new tools for managing compliance and monitoring financial reporting processes (Jeyasingh, 2023). Regulatory Technology systems use automated monitoring systems, data analytics systems, and artificial intelligence systems that facilitate compliance services (anti-money laundering detection, suspicious activity reporting, and transaction monitoring).

In recent years, the uptake of these systems has been increasing at a very high rate. According to industry reports, there is an increase in investment in Regulatory Technology solutions by financial institutions striving to cope with the rising complexity in regulatory requirements (Jeyasingh, 2023). There is evidence that automated compliance systems can minimize financial reporting errors by about 20 to 30 percent and enhance reporting efficiency by reducing financial closing cycles (Azubuike, 2024). Audit preparedness is also enhanced with the help of Regulatory Technology tools, which serve to keep the digital records of compliance activities and financial transactions on a constant basis. The automated documentation lowers the burden of manual recordkeeping, as well as enables firms to respond faster to regulatory reviews and audits.

Nevertheless, there is also a risk of governance issues when advanced compliance technology is adopted. With the growing complexity of risk management systems, the corporate audit committees might be under great pressure to manage technological risks that demand specialized skills (Ashraf *et al*., 2024). These dynamics underscore the need to strengthen the governance structures as well as the adoption of technology (Tetteh-Kpakpah *et al*., 2025).

DISCUSSION

The results of this paper demonstrate the current transformation in cybersecurity disclosure among the financial reporting framework of U.S. public firms and the impact of these practices on capital markets transparency. The evidence indicates that the recent regulatory changes have institutionalized cybersecurity disclosure as part of corporate reporting (U.S. Securities and Exchange Commission, 2023). Mandatory reporting requirements have encouraged firms to incorporate cybersecurity governance and incident management into their financial reporting structures (Swift & Colon, 2024). Nevertheless, as

Publisher: SARC Publisher

the disclosure practices have become standard, the quality and clarity of the disclosed information are still uneven (Swift & Colon, 2024). In a number of situations, the disclosures are based on generalized language, which gives less information about how the firms handle digital risks, making the information less useful to investors and regulators. It is also shown that the investors are paying more attention to cybersecurity risk as a recurring operational risk instead of an isolated incident (Charoen & Khern-am-nuai, 2025). The available empirical evidence also indicates that less sensitivity of the market to announcements of cyber breaches may be indicative of capital markets becoming accustomed to the occurrence of these events (Charoen & Khern-am-nuai, 2025). Nevertheless, the impact of cybersecurity events remains significant when breaches involve sensitive data exposure or operational disruptions (Bederna & Szádeczky, 2023). In these instances, the reaction in the market still shows that there is a concern over governance failures, financial reporting reliability, and reputational damage (Issayeva *et al*., 2023). These findings support the argument that cybersecurity disclosure practices play an important role in shaping investor perceptions of corporate risk management.

The other important observation of the findings is linked to the impact of internal control systems on the credibility of cybersecurity disclosures. The issue of persistent material weaknesses in internal control over financial reporting is a significant governance concern (Tian *et al*., 2025). The fact that a significant percentage of material weaknesses continue over a period of several years demonstrates that not all organizations are capable of ensuring effective monitoring of complex information systems (Tian *et al*., 2025). With weak internal control systems, the credibility of financial disclosures, such as cybersecurity reporting, can be undermined (Elsayed & Elshandidy, 2021). Additional audit fees and delays in reporting due to the continued existence of control weaknesses are another indication of the operational difficulties that firms experience when their financial reporting systems are not effectively supported by proper governance structures (Fischer *et al*., 2020). The results also put an emphasis on the increasing role of regulatory technology in aiding financial reporting and compliance monitoring. Regulatory reporting requirements and identification of anomalies in financial transactions are becoming components managed through automated monitoring systems, data analytics platforms, and compliance systems based on artificial intelligence. The fact that there is evidence of a decline in financial reporting errors and enhanced reporting efficiency indicates that these technologies can make financial reporting processes more reliable (Azubuike, 2024). Regulatory Technology systems enhance the capacity of the firms to detect possible reporting problems and to react faster to regulatory investigations by allowing continuous monitoring and keeping digital audit trails.

Although such benefits exist, the implementation of advanced compliance technologies presents new governance issues. As digital monitoring systems become more sophisticated, corporate boards and audit committees face increasing difficulty in overseeing technology-driven risk management systems. This trend, commonly referred to as "audit committee overload," is an indication of the widening range of duties owed to governance authorities in charge of financial management (Ashraf *et al*., 2024). Traditional financial reporting-driven committees are required today to take up cybersecurity risks, data governance concerns, and new technological advancements like artificial intelligence. In the absence of adequate technical skills at the board level, monitoring of these systems can be excessively reliant on external audit and technology advisors (Velte, 2023). Considering the findings at a larger scale, it is implied that the issue of cybersecurity governance concerns not just the individual companies but also the stability of the financial markets. Cybersecurity threats are also becoming a recognized area of concern to policymakers as a potential systemic threat to financial infrastructure (Financial Stability Oversight Council, 2025; Bonsu, 2025). Financial stability authorities' reports demonstrate how ripple effects across the financial system could be caused by disruption in systemically important financial institutions or other crucial service providers (Financial Stability Oversight Council, 2025). As a result, regulatory frameworks increasingly emphasize operational resilience, requiring firms to strengthen risk monitoring, disclosure practices, and incident response capabilities (Bohn & Schiereck, 2023).

Combined, these results demonstrate the need to include cybersecurity governance in financial reporting systems. Effective cybersecurity disclosure practices require a combination of transparent reporting, strong internal control systems, and reliable monitoring technologies (Laryea & Brakye, 2025). When the elements are

Publisher: SARC Publisher

combined, firms are well positioned to deliver correct and timely information regarding digital risks, which enhances transparency and accountability within capital markets. On the other hand, poor internal controls, less disclosure detail, and the lack of governance oversight can erode investor confidence and lower the effectiveness of cybersecurity reporting. The discussion therefore supports the central argument of this study: *cybersecurity disclosure practices contribute to financial reporting transparency when they are supported by credible governance mechanisms and effective monitoring systems*. With the ongoing transformation of the financial reporting process by digital technologies, organizations need to change the nature of their governance frameworks to guarantee that cybersecurity threats are detected, tracked, and reported in a manner that preserves the integrity of corporate reporting and the confidence of market participants (Tetteh-Kpakpah *et al*., 2025).

IMPLICATIONS

Implications of Financial Governance

The results of this study point to several implications of financial governance in organizations that operate in more digital financial reporting settings. With cybersecurity risks already connected with financial reporting systems, governance frameworks need to transform in a way that allows digital risks to be monitored, controlled, and disclosed appropriately (Velte, 2023).

For Boards of Directors

The findings show that there is an increasing demand for technical competence among corporate boards, especially among audit committees, which have a role in supervising financial reporting and internal control. The occurrence of cybersecurity incidents and digital reporting risks is increasingly impacting the integrity of corporate disclosures, and several boards still depend on external auditors and external cybersecurity consultants to provide guidance. Even though external expertise is essential, overreliance on external advisors may create governance gaps where boards are not equipped with the internal capabilities to assess technology-related risks on their own. Enhancing the cyber competencies of audit committees can enhance the management of internal control systems, cybersecurity risk management, and disclosure practices mandated by current regulatory frameworks (Ashraf *et al*., 2024).

For Audit Professionals

The results also indicate that the auditing profession will have to keep evolving its practices in order to deal with the technology-driven financial reporting risks. Conventional audit methods are based on retrospective testing of financial information at periodic intervals. Nevertheless, increased reliance on automated reporting systems and digital platforms of transactions necessitates auditors to implement more continuous monitoring methods. By incorporating artificial intelligence and data analytics into auditing procedures, irregular transactions and anomalies in financial data, as well as possible compliance failures, could be detected in real-time. These tools can enable auditors to enhance control over the complex reporting environments and enhance the reliability of financial disclosure (Velte, 2023).

For Corporate Management

Corporate leadership will also have to take a more active role in the governance of cybersecurity as digital risks continue to overlap with the financial reporting requirements. Regulation S-K Item 106 disclosure requirements demand that companies explain how they handle and govern cybersecurity risks in the organization (U.S. Securities and Exchange Commission, 2023). Consequently, cybersecurity risk management is not only restricted to technical departments but has also become a financial reporting responsibility. The role of Chief Financial Officers and top financial executives in the organization is becoming more relevant in the coordination of cybersecurity governance, preparation of disclosures, and regulatory compliance. The collaboration between the finance teams, information security leadership, and compliance departments should be effective to make sure that cybersecurity incidents are adequately assessed, reported, and disclosed in the financial filings.

On the whole, the results indicate that the enhancement of financial governance in the digital age needs more interconnection of cybersecurity management, internal control frameworks, and financial reporting procedures. Companies that enhance the expertise of boards, implement technology-enabled auditing procedures, and engage financial leadership in cybersecurity governance are in a better position to ensure the credibility and transparency of their financial reporting systems (Laryea & Brakye, 2025).

Publisher: SARC Publisher

Implications on Policy and Regulations.

This research also has significant consequences for regulatory bodies whose role is to ensure transparency and stability in capital markets. With cybersecurity risks having a growing impact on financial reporting systems, regulators have to continue refining disclosure criteria and governance expectations to ensure that investors get transparent and reliable information related to digital risks (U.S. Securities and Exchange Commission, 2023; Financial Stability Oversight Council, 2025).

A major implication is related to the quality and usefulness of cybersecurity disclosures. Although more recent regulatory demands have enhanced the timeliness of cybersecurity reporting, the results indicate that the informativeness of qualitative disclosure is not consistent across the firms. Most companies meet disclosure obligations through generalized or standardized language that does not give much information on the nature of cybersecurity risks or governance mechanisms applied to address them (Swift & Colon, 2024). Regulators might have to put more emphasis on enhancing the transparency and readability of cybersecurity reporting in a way that allows investors to have a better understanding of the operational and financial repercussions of cyber threats.

Another implication is associated with the increased adoption of automated compliance systems and regulatory technology within financial institutions. With more organizations turning to artificial intelligence and automated surveillance to help them maintain regulatory compliance, policymakers might have to come up with more explicit regulations on how these systems should be governed and held to account (Bonsu, 2025). Transparency-enhancing models in the design, monitoring, and validation of automated compliance tools can be applied to keep such technologies functioning in a reliable, explainable, and regulatory-compliant manner. A better definition of the expectations of responsible use of compliance technologies would also assist regulators in assessing the manner in which firms undertake digital risk monitoring in financial reporting settings (Jeyasingh, 2023).

Another requisite issue is interjurisdictional regulatory coordination. Most cybersecurity incidents are supposed to be reported in accordance with a variety of regulations, including federal disclosure and state-level breach notification policies (Bohn & Schiereck, 2023). The difference in reporting requirements, schedules, and definitions of material events can lead to inconsistency in reporting cybersecurity incidents to investors and regulators. Increased coordination of federal disclosure rules with state reporting requirements would be beneficial in reducing uncertainty in the reporting process and in making sure that investors obtain more consistent information on cybersecurity incidents impacting publicly traded firms.

Finally, regulators may need to regularly deal with the interaction of cybersecurity risks with systemic financial stability concerns. As more financial institutions become more interconnected through digital infrastructure, the impact of cybersecurity incidents may transcend beyond the organizational scope of a single organization (Financial Stability Oversight Council, 2025). Enhancement of disclosure requirements, responsible use of compliance technology, and better coordination of regulatory authorities can, therefore, be significant in ensuring transparency and robustness in the contemporary financial markets.

Altogether, the results imply that efficient regulatory frameworks should keep changing in tandem with technological change. Through better disclosure advice, promotion of responsible implementation of compliance technology, and more robust coordination between regulatory systems, policymakers can increase the transparency of the cybersecurity governance system and contribute to the integrity of financial reporting in the digital economy.

CONCLUSION

Technology-driven risk governance has become essential in financial reporting transparency in U.S. capital markets. With the growing digitalization of corporate reporting systems, cybersecurity threats are directly related to the credibility of the financial disclosures, internal control systems, and investor confidence. Results of this study indicate that regulatory changes, especially the establishment of mandatory cybersecurity disclosure policies, have enhanced the presence of cyber risk in corporate reporting. Simultaneously, an increase in the use of regulatory technology has enhanced monitoring, compliance, and accuracy of financial reporting processes. Nonetheless, the findings also demonstrate that there are still significant governance issues. The consistent internal control vulnerabilities still erode the reliability of

Publisher: SARC Publisher

reporting in certain companies, whereas the growing technological complexity puts a heavier burden on boards and audit committees expected to oversee financial accountability. The findings indicate that it is necessary to enhance the integration of cybersecurity governance, internal control systems, and financial reporting practices. Comprehensively, cybersecurity disclosure, together with credible monitoring technologies, can enhance transparency and accountability in capital markets. Enhancing governance capability and optimizing regulatory directions is still essential in ensuring financial reporting mechanisms are not compromised in delivering transparent and reliable information in a more digitalized financial setting.

REFERENCES

1. Ashraf, M., Choudhary, P., & Jaggi, J. "Are audit committees overloaded? Evidence from the effect of financial risk management oversight on financial reporting quality." *Management Science* 70.12 (2024): 8414-8447.
2. Azubuike, J. I. "The Role of Predictive Analytics in Automating Risk Management and Regulatory Compliance in the US Financial Sector." *EUROPEAN JOURNAL OF ACCOUNTING, AUDITING AND FINANCE RESEARCH Учредители: European Centre for Research Training and Development* 12.10 (2024): 19-31.
3. Bederna, Z., & Szádeczky, T. "Managing the financial impact of cybersecurity incidents." *SECURITY DEFENCE QUARTERLY* 41.1 (2023): 1-21.
4. Bohn, L., & Schiereck, D. "Regulation of data breach publication: the case of US healthcare and the HITECH act." *Journal of Economics and Finance* 47.2 (2023): 386-399.
5. Brakye, K., & Adam, A. B. K. "CYBERSECURITY RISK DISCLOSURE AND REGULATORY COMPLIANCE: EVALUATING MARKET SENSITIVITY AND DISCLOSURE EFFECTIVENESS IN US PUBLIC COMPANIES."
6. Cao, H., Phan, H. V., & Silveri, S. "Data breach disclosures and stock price crash risk: Evidence from data breach notification laws." *International Review of Financial Analysis* 93 (2024): 103164.
7. Charoen, D., & Khern-am-nuai, W. "Revisiting the (disappearing) cost of data breach disclosures." *Digital Policy, Regulation and Governance* 27.1 (2025): 37-55.
8. Elsayed, M., & Elshandidy, T. "Internal control effectiveness, textual risk disclosure, and their usefulness: US evidence." *Advances in accounting* 53 (2021): 100531.
9. Financial Stability Oversight Council. "2025 annual report." *U.S. Department of the Treasury.* (2025).
10. Fischer, B., Gral, B., & Lehner, O. "SOX section 404 twenty years after: Reviewing costs and benefits." *ACRN Journal of Finance and Risk Perspectives (JOFRP)* 9.1 (2020): 103-112.
11. Fischman, H., Reisner, L., & Carey, J. "SEC enforcement: 2025 year in review." *Harvard Law School Forum on Corporate Governance*. (2026).
12. Issayeva, G. K., Zhussipova, E. E., Aitymbetova, A. N., Kuralbayeva, A. S., & Abdykulova, D. B. "The Impact of Cybersecurity Breaches on Firm's Market Value: the Case of the USA." *Economy: strategy and practice* 18.4 (2024): 200-219.
13. Jeyasingh, B. B. F. "Impact of RegTech on compliance risk due to financial misconduct in the United States banking industry." *Digital Economy and Sustainable Development* 1.1 (2023): 24.
14. Jiang, W., Xu, C., & Counts, R. W. "XBRL reporting in firms with data breach incidents." *Journal of Corporate Accounting & Finance* 35.3 (2024): 146-156.
15. Laryea, J. E. N., & Brakye, K. "Modernizing general ledger reconciliation standards: Reducing systemic risk in financial reporting across public and private sectors." *Sarcouncil Journal of Economics and Business Management*, 4.10 (2025): 1–7.
16. Bonsu, M. A., & Akekudaga, P. "Enhancing Critical Infrastructure Security: Addressing Cybersecurity Risks and Regulatory Gaps in AI-Enabled IoT Systems." *2025 IEEE 16th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE, (2025).
17. Swift, O., & Colon, R. "A Content Analysis of the Modernization of Regulation SK Items 101, 103, and 105." *Journal of Applied Business & Economics* 26.6 (2024).
18. Tetteh-Kpakpah, C., Adjaottor, S., & Donkor, A. "Mitigating cyber threats through cybersecurity audits and adaptive defense: A case study on financial institutions." *EPRA International Journal of Economic and Business Review*, (2025): 12–16.

Publisher: SARC Publisher

19. Tian, T., Mei, S., & Tang, T. "Persistent internal control failures: Examining multiple consecutive years of disclosing material weaknesses." *Journal of Corporate Accounting & Finance* 36.1 (2025): 105-123.
20. Tosun, O. K. "Cyber-attacks and stock market activity." *International Review of Financial Analysis* 76 (2021): 101795.
21. Securities, U. S., & Exchange Commission. "SEC adopts rules on cybersecurity risk management, strategy, governance, and incident disclosure by public companies." *Jul* 26.2023 (2023): 2023-139.
22. Velte, P. "The impact of external auditors on firms' financial restatements: a review of archival studies and implications for future research." *Management Review Quarterly* 73.3 (2023): 959-985.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Brakye, K. & Yeboah, M. M. "Technology-Driven Risk Governance in U.S. Financial Reporting: The Role of Cybersecurity Disclosure and Regulatory Technology in Strengthening Capital Market Transparency" *Sarcouncil Journal of Engineering and Computer Sciences* 5.4 (2026): pp 107-117.

Publisher: SARC Publisher