Research Paper

EPRA International Journal of Economic and Business Review-Peer Reviewed Journal
Volume - 13, Issue - 7, July 2025 | e-ISSN: 2347 - 9671| p- ISSN: 2349 – 0187

SJIF Impact Factor (2025): 8.862 || ISI Value: 1.433 || Journal DOI URL: https://doi.org/10.36713/epra2012

MITIGATING CYBER THREATS THROUGH CYBERSECURITY AUDITS AND ADAPTIVE DEFENSE: A CASE STUDY ON FINANCIAL INSTITUTIONS

Clement Tetteh-Kpakpah [a], Solomon Adjaottor [b], Alice Ama Donkor [c]

[a] *Temple University, Pennsylvania (PA) / Fox School of Business, IT Auditing and Cybersecurity, USA*
[b] *Department of Accounting and Finance, Kwame Nkrumah University of Science and Technology, Ghana*
[c] *Department of Computer Science, Kwame Nkrumah University of Science and Technology, Ghana*

***Corresponding Author**: Alice Ama Donkor*

ABSTRACT DOI No: 10.36713/epra23002 Article DOI: https://doi.org/10.36713/epra23002

The financial sector, specifically institutions operating in capital markets, remains a prime target for evolving cyber threats due to its heavy reliance on interconnected digital systems today. This study examines the role of cybersecurity audits and adaptive defense mechanisms in mitigating these threats, using financial institutions as a case study. Cybersecurity audits play a critical role in identifying vulnerabilities, ensuring regulatory compliance, and strengthening organizational defenses. Adaptive defense strategies, such as AI-driven monitoring and real-time threat mitigation, enhance the effectiveness of these audits. By analyzing case studies and assessing audit methodologies, this research underscores the significance of integrating cybersecurity audits with adaptive measures to safeguard sensitive financial data and preserve the operational integrity of financial institutions. The findings highlight the necessity of robust and dynamic cybersecurity practices in fostering financial system resilience, protecting stakeholder confidence, and contributing to economic stability.

KEYWORDS: ***Cybersecurity Audits, Adaptive Defense, Financial Institutions, Risk Mitigation, Resilience***

INTRODUCTION

U.S. capital markets stand as the largest, most liquid, and most influential in the world, acting as both the heart of the U.S. financial system and a driver of the global financial system. The U.S capital market is unique in the way that it provides larger percentages of funding for businesses compared to the normal banking sectors, which makes it vital for the growth of the economy (Raedle, 2022). These markets are mainly intertwined with the financial well-being of organizations as well as individuals, providing investment across a spectrum of asset classes, from equities and debt to derivatives. Not only do they provide capital for businesses ranging from small enterprises to large corporations, but they also offer risk management strategies in different sectors through their products, such as derivatives. In addition, securitization markets in the U.S are important in credit channels, especially credit cards, automobile loans, and mortgages that enhance access to financial products. Embedded in these markets is a strong financial infrastructure, including clearing and settlement operations that support the effective functioning of these complex systems. Presenting a market value of equity in $29 trillion, $14 trillion in US treasury securities, and corporate bonds that are more than $8 trillion, the US capital market is one of the leading enablers of economic opportunities and global investment (US Department of the Treasury, 2017). The broad participation of investors, ranging from the huge industry players to the small investors, clearly shows the deep and global reach of these markets, which operate around the clock continuously across financial centers throughout the world.

Although the US capital markets have always been considered the power of the global economy, their integration and increased dependence on technology have brought one more risk factor – cybersecurity (Ashish et al., 2024). With more financial transactions moving to the online space, the risk of cyberattacks on market structures, financial institutions, and private investors has risen dramatically. Cybercriminals, state-sponsored actors, and other information threats are growing smarter with the singular goal of compromising organizational operations, stealing sensitive data, and eroding investor confidence. This has given rise to the urgent need to protect these important systems through the implementation of an effective system that would ensure their continued functionality as well as protect investors' confidence.

Cybersecurity audits have become widely utilized in the protection of the U.S. capital markets against these new-age threats. These audits are crucial in their capacity to offer a

comprehensive and methodical analysis of an organization's cybersecurity practices, with the aim of answering the kind of questions relevant to the assessment of compliance with regulations aimed at preserving marketplace integrity. These audits do more than test an institution's cybersecurity threat identification and response capabilities. They ensure compliance with regulatory standards, for example those set by the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA). Such compliance is paramount as failure to adhere to these frameworks has led to companies suffering significant financial and reputational losses.

Based on this, this paper aims to identify the impacts of cybersecurity audits in the US capital markets, especially in improving the security and stability of financial systems. This study looks at the criteria used in these audits, the issues that organizations encounter in implementing and maintaining cybersecurity standards, and the important balance between promoting growth opportunities and ensuring financial stability. Through a discussion and analysis of these elements, this paper highlights the importance of the ongoing enhancement of audit practices and related legal frameworks to protect both market stakeholders and the broader economy.

Cybersecurity audit refers to a comprehensive analysis of an organization's IT systems, standards, and measures aimed at determining their adequacy in protecting against cyber threats (Krishna, 2023). According to the SecurityScorecard, a cybersecurity audit serves as a checklist to validate that all the security mechanisms claimed by an organization correspond to being in place and functioning effectively (SecurityScorecard, 2020). This process not only identifies risks but also ensures compliance with necessary legal requirements and standards. The Federal Financial Institutions Examination Council (FFIEC) highlights the importance of such audits being vital in managing cybersecurity risks, hence improving the overall security posture of organizations (FFIEC, 2017). Cybersecurity audits other than compliance objectives involve identifying weaknesses in security controls, examining the efficiency of response to cyber threats, and offering recommendations for enhancement. ISACA notes that as cyber threats are on the rise, it is vital for IT auditors to understand cybersecurity practices, reinforcing the role of audits in preserving organizational integrity (ITAF, 2020).

Financial institutions form an integral part of the capital market ecosystem, and the probability of their exposure to cyber risks poses significant risks. A successful cyber-attack can result in loss of business through interruption of transactions, loss of confidential information, and erode investors' confidence. With the average cyber insurance claim rising from USD 145,000 in 2019 to USD 359,000 in 2020, there is a growing necessity for better cyber information sources, standardized databases, mandatory reporting, and public awareness (Cremer et al., 2022).

Also, the financial markets of the world are interconnected, which results in the fact that vulnerabilities in one institution are likely to cause risks to many more institutions. For instance, when investors trust that their information is safe given high levels of cybersecurity, they are more likely to confidently participate in the markets. On the other hand, breaches can negatively affect the perception of investors, specifically lowering market liquidity and increasing fluctuations within capital markets. Therefore, maintaining good cybersecurity is not only a function of safeguarding individual institutions but also a need for the financial system's stability.

The regulatory landscape governing cybersecurity audits is characterized by several key frameworks and guidelines. The Securities and Exchange Commission (SEC) mandates that public companies report material risks related to cybersecurity incidents. (Mohammed, 2015). This requirement directly emphasizes the importance of transparency and accountability in managing cyber risks, which requires organizations to demonstrate how they are preventing cybersecurity threats and protecting investors from potential risks. Additionally, the Financial Industry Regulatory Authority (FINRA) outlines general and specific recommendations for member firms on how to implement effective cybersecurity measures. With particular reference to the importance of periodic audits, FINRA highlights their importance in approaching compliance with set security standards and managing risks adversely. This approach is in line with the increasing understanding that regular assessment is critical when it comes to preserving financial integrity in conditions of the constant threat of influence (Carter and Zheng, 2015). Another critical regulation is the Gramm-Leach-Bliley Act (GLBA) that requires financial institutions to protect consumers' financial data through comprehensive security programs, including regular audits to determine compliance with privacy provisions from time to time. These regulatory requirements highlight the importance of cybersecurity audits as a way of ensuring that financial institutions meet the legal requirements while improving overall security at the same time (Mohammed, 2015).

Understanding the theoretical fundamentals of cybersecurity audits is essential for recognizing the importance of protecting the U.S capital market. As new and more complex cyber threats are emerging, the frameworks within which these audits are established also need to evolve and adapt to ensure adequate and effective risk mitigation for these critical financial structures.

Identifying Risks and Vulnerabilities

Cybersecurity audits are integral in identifying vulnerabilities in financial systems. These audits involve a detailed assessment of the infrastructure of an organization, its policies and operational activities, and identify gaps that may include unpatched software, misconfigured systems, or outdated protocols (Lois et al., 2021). Such vulnerabilities are potential starting points of cyberattacks, which is why identifying them is a first step to risk mitigation. In addition, cybersecurity audits utilize sophisticated techniques and frameworks that make sure that, in addition to discovering new exposures that may not be revealed during ordinary business activities, organizations can prevent security breaches. Current studies note that third-party integration vulnerabilities and supply chain risks are increasingly targeted by attackers (Li and Xu, 2021). Cybersecurity audits that focus on such areas can minimize risks to a very large degree, especially within the complex network of capital markets. In this manner, cybersecurity audits enable financial institutions to identify these potential risks and

apply specific countermeasures that improve the security of their processes.

Ensuring Compliance

The laws governing the U.S. capital markets place stringent requirements when it comes to protecting financial institutions from cybersecurity threats. Conducting cybersecurity audits proves to be the most appropriate measure to ensure compliance with these regulatory requirements. These standards interpret how risk management, information sharing, and data protection are essential to ensuring comprehensive cybersecurity measures for financial institutions. Failure to adhere to these frameworks may attract severe penalties, damage to reputation, and operational disruption, highlighting the importance of cybersecurity audits in managing regulatory risks. The Federal Information Security Modernization Act (FISMA) sets security requirements for federal agencies and their contractors, emphasizing the protection of critical data through systematic audits and controls. Originally, this Act was designed for the government organization, but its conceptual models have influenced the private sector practices, especially in the financial sector (Mohammed, 2015). In the same way, the Payment Card Industry Data Security Standard (PCI DSS) is an industry-recognized standard that enforces strict measures for securing cardholder data, with cybersecurity auditing serving as a vital component for maintaining compliance and for assessing vulnerabilities in data security protocols (Bhutta et al., 2022). In addition, the Cybersecurity Information Sharing Act (CISA) promotes collaboration between private and government organizations. (Oluomachi et al., 2024) assert that organizations that consistently prioritize compliance through regular cybersecurity audits exhibit enhanced risk management capabilities, which in turn confer a distinct competitive advantage in the marketplace. Compliance-driven audits go beyond just adherence to regulations. They help to create an organizational culture of transparency and accountability. In evaluating cybersecurity measures against these diverse frameworks systematically, cybersecurity audits assist financial institutions in identifying deficiencies, implementing robust response actions, and adapting continuously to the evolving threat landscape.

Case Study

No organization is immune to cyberattacks. Even the best-protected financial organizations can become victims of cybercriminals despite significant investments in cybersecurity. Cybersecurity awareness is not only crucial but essential in safeguarding our businesses from such risks. In line with this, (Jadhav, 2023) established conclusively in his assessment of Cybersecurity Audits' Function in Managing Business Applications and Systems in the United States that different risks, vulnerabilities, and threats are identified and affect critical domains. He provided unequivocal evidence that cybersecurity audits play a crucial role in detecting risks, vulnerabilities, and threats faced by organizations, impacting various vital domains, including network security, system security, data security, operational security, and physical security.

In 2016, the hackers stole the PIN and user ID of an employee of Bangladesh Bank and installed six types of malware on its IT system. As soon as they went through a series of test runs, logging into the bank's system several times, they added extra surveillance software and erased files from databases. The hackers then used the access they had gained to the SWIFT system to send payment requests to Bangladesh Bank's account at the Federal Reserve Bank of New York (NY Fed). Because these payment requests from Bangladesh Bank were odd, that is, the names of the correspondent banks required were missing in all the messages, the transfers were not executed automatically. Furthermore, the amount involved was very large, and most payments were made to individual accounts rather than the institutions. It followed that after 35 messages had been rejected because of improper formatting, the hackers simply fixed that and resent the emails. This time, five payment requests, which amounted to $81 million in total, were made, with the money being transferred to accounts in the Philippines. The funds were then channeled to accounts at the Rizal Commercial Banking Corporation (RCBC) bank in Manila, which disappeared into the Philippine casino system that is exempted from the country's anti-money laundering regulations. The hack was successful because the culprits were able to delete the fraudulent transcriptions from Bangladesh Bank's records. They also interfered with message transmission between Bangladesh Bank and the NY Fed, hence, NY Fed's queries and alerts never got to the Bank (Gopalakrishnan and Mogato, 2016).

Most banks take special precautionary measures for computers with access to SWIFT. Multiple firewalls are created to isolate the system from other bank networks, with these computers in separate, locked rooms. The investment on the part of the Bangladesh Bank in cybersecurity was found to be lower than the requirements of other central banks. According to news reports, they employed unsophisticated routers and did not establish any firewalls. Further, the transaction monitoring system of the NY Fed was unable to detect the anomalies in real time as it analyzes payments only after payments are made (Varadhan, 2018). On these occasions, SWIFT claims that its system was not compromised. However, with financial security experts highlighting that the SWIFT system can only be as strong as its weakest link, SWIFT now requires its users to regularly report on the status of their security infrastructure (Paulus, 2018).

How Cybersecurity Audits Could Have Mitigated Damage

The Bangladesh Bank heist reveals just how critical comprehensive cybersecurity audits are in averting such devastating breaches. Such significant vulnerabilities could have been detected and reported in the bank's cybersecurity posture, such as the absence of firewalls and the use of outdated routers during a cybersecurity audit. These deficiencies indicate non-compliance with standard security protocols, which would have been detected and addressed by appropriate security audits. Additionally, audits could have evaluated the effectiveness of the bank's monitoring systems and consequently identified the inadequacy of the transaction monitoring system, which failed to detect the anomalies in real time. Had proactive cybersecurity audits been made, recommendations for implementation of real-time monitoring tools as well as multi-factor controls to minimize access to SWIFT messages were raised. Moreover, more often than not, cybersecurity audits simulate attacks to test the preparedness of the system. Some of those tests could have possibly revealed Bangladesh Bank's IT infrastructure vulnerability to malware and other spyware to

help the bank take preemptive measures. Furthermore, cybersecurity audits are specifically focused on the incident response of an organization. In this case, the bank's failure to detect and respond to message interference and fraudulent transcription deletion defines the bank as an organization that presents a lack of operational readiness. Cybersecurity audits could have required the adoption of an efficient incident response plan, ensuring that the bank can effectively contain and remediate breaches. Therefore, such a cybersecurity audit would not only have given the bank a better defense posture against such sophisticated cyber threats, but also a better capability to detect, respond and mitigate them.

Adaptive Defense

While cybersecurity audits are important for the assessment of risk and compliance, their findings must be incorporated with adaptive defense mechanisms. Proactive defense measures include constant surveillance and artificial intelligence-driven threat detection systems that provide dynamic countermeasures to complex cyber threats. For instance, if Bangladesh Bank had adopted AI-based anomaly detection systems, the suspicious transaction patterns and irregularities in SWIFT payment requests would have been detected and flagged before execution. These systems monitor behavior and notice any anomaly, providing immediate alerts for investigation. In the same way, real-time monitoring tools could intercept the hackers' movements during their reconnaissance phase, including planting or installing malware and surveillance applications. Continuous monitoring would have identified the unauthorized access and immediately isolated the compromised systems. Another key aspect of adaptive defense is the integration of threat intelligence. Bangladesh Bank could have leveraged information from similar cyberattacks on financial organizations to harden its defense against the identified tactics, techniques, and procedures (TTPs). This approach would have minimized the probability of a successful breach. Audits and adaptive defenses work in partnership to generate several layers of security. Whereas audits reveal poor structures and recommend improvements that may be needed, adaptive measures give flexibility to deal with real-time threats. Combined, they strengthen the defense of financial institutions against traditional and evolving cyber threats that threaten systems and data among United States financial institutions.

The Verizon 2024 Data Breach Investigations report reveals that the financial and insurance sectors have become more elaborate and diverse in terms of cyber threats, where system intrusions now surpass miscellaneous errors, and basic web application attacks are the primary attack vector. This shift shows the change of modus operandi of threat actors, including an increase in the use of social engineering that targets human beings as much as it targets technical systems. The report reveals that 78% of the breaches originate from three dominant patterns, namely system intrusion, miscellaneous errors, and social engineering. Moreover, more than half of these breaches stem from external actors, which account for 69%, while threats from insiders also remain significant at 31%, proving that systems need security from both external and insider threats. In this respect, cybersecurity audits are indispensable in the protection of the United States' capital markets. Regular audits are central to vulnerability identification, compliance checks, and ensuring that all potential threat agents from both outside and inside the organization are comprehensively addressed. Audits provide financial institutions with proactive measures to address the ever-evolving threat landscape by uncovering weaknesses and enhancing resilience, thereby protecting personal information, bank records, and credentials from compromise (Verizon, 2024).

Limitations of Current Practices

The audit process, when effectively executed, ensures accountability, enhances transparency, and strengthens the confidence of the stakeholders in the cybersecurity practices of an organization. Bangladesh Bank shows an example of how a lack of efficient cybersecurity auditing enabled the vulnerabilities exploited in the attack. Despite this, current audit practices are not without their drawbacks. First, audits are often done at intervals other than continuous, and organizations are at the mercy of evolving threats during these non-audit intervals. Attackers increasingly use sophisticated methods such as social engineering and zero-day exploits, which may bypass conventional audit findings if such techniques appear after the audit has been completed. Furthermore, most audit processes rely on compliance checklists, unlike a dynamic analysis of threats, which fails to adequately respond to novel attack vectors. Another considerable challenge is the issue of resource distribution. Quite often, Small and medium-sized financial institutions lack the funds and technical expertise to implement comprehensive audit recommendations. Additionally, audits sometimes fail to integrate with broader cybersecurity strategies, which results in fragmented defenses leaving critical gaps unaddressed. Such limitations necessitate the development of improved audit strategies that are adaptive, proactive, and continuous.

Recommendations and Future Directions

Current approaches to cybersecurity audits need to become more effective due to the emergence of new threats and the growing level of risk, particularly in the financial sector. A key recommendation concerns the implementation of continuous auditing practices. As opposed to periodic audits, continuous audits give institutions the ability to monitor systems in real time, enabling institutions to detect vulnerabilities and threats as they emerge. This approach ensures a proactive posture towards cyber threats and is consistent with the use of adaptive defense measures. The adoption of continuous auditing in combination with automated tools can help minimize response time to the identified anomalies, hence prevent damages.

One of the most important areas that needs to be developed is the combination of cybersecurity audits with adaptive defense systems. Auditing often reveals weaknesses and gaps in an organization's defense systems, but no corresponding real-time solutions to these findings. Adaptive defenses, such as artificial intelligence-driven threat identification and behavioral analytics, enable a dynamic approach to act on audit findings. In circumstances where audits reveal exposures regarding unpatched systems, adaptive systems can promptly address these by prioritizing the necessary updates to these systems or by isolating such systems from the network to reduce threat impact. Furthermore, the training of the workforce cannot be ignored in improving the effectiveness of cybersecurity audits. Human errors, including those exploited through social engineering attacks, are some of the risks that organizations

cannot fully neutralize. It is therefore important that organizations incorporate training programs aligned with audit recommendations to enhance the employee's awareness and responses to threats. Financial institutions could consider using the audit findings to develop training sessions which would help to fill the gaps such as poor password management or the laxity with lapses in email security protocols. which emails are managed. Lasty, it is crucial to have an international form of standardization of cybersecurity audits amongst the interconnected financial ecosystem. While financial transactions and operations transcend national borders, inconsistent audit standards introduce a vulnerability that attackers can capitalize on. To increase the global resilience of systems, globally accepted frameworks and standards have to be established, and encouraging cooperation in sharing audit findings and threat intelligence will contribute to promoting a more resilient financial ecosystem.

CONCLUSION

This paper highlights the importance of cybersecurity audits and the use of adaptive defense strategies to mitigate the increasing threats faced by financial institutions. Cybersecurity audits are a structured approach to identifying vulnerabilities, ensuring regulatory compliance, as well as setting up a reference point for managing risks in the cyber environment proficiently. Supported by adaptive defense mechanisms like the use of artificial intelligence in threat identification and constant monitoring, these audits evolve from being static assessments into proactive tools in enhancing cybersecurity.
The evaluation of case studies shows the practical application of these measures, demonstrating how their implementation minimizes the occurrence and scale of cyber threats.

However, the research also identifies gaps associated with audit implementation and the adoption of adaptive strategies, which require further attention in line with the current evolving threat landscape. Going forward, financial institutions have to prioritize continuous improvements to constantly enhance their audit methodologies and integrate advanced defense systems to ensure stability for operations, security of data and reliability in the financial ecosystem.

By bridging the strengths of traditional audits together with the capabilities of today's innovative, flexible and adaptive technologies, the financial sector can sufficiently address the challenges of contemporary cyber threats and provide financial sustainability in the conditions of the evolving digital environment.

REFERENCES

1. *US Department of the Treasury (2017) A Financial System That Creates Economic Opportunities, Capital Markets. Report to President Donald J. Trump, Executive Order 13772 on Core Principles for Regulating the United States Financial System.*
2. *Raedle D. (2022). Understanding the U.S. Capital Market Structure for Capital Raising Success. Deer Isle Group, LLC*
3. *Juneja, Ashish & Goswami, Shankha & Mondal, Surajit. (2024). Cyber Security and Digital Economy: Opportunities, Growth and Challenges. Journal of Technology Innovations and Energy. 3. 1-22. 10.56556/jtie.v3i2.907.*
4. *Jadhav, Krishna. (2023). THE ROLE OF CYBER SECURITY AUDITS.*
5. *SecurityScorecard (2020) What Is a Cybersecurity Audit and Why Does it Matter? Available at: https://securityscorecard.com/blog/best-practices-for-a-cybersecurity-audit/*
6. *FFIEC (2017) Cybersecurity Assessment Tool.*
7. *IT Audit Framework (ITAF™) (2020) Professional Practices Framework for IT Audit.*
8. *Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F, Materne S. (2022) Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract. 47(3):698-736. doi: 10.1057/s41288-022-00266-6. Epub 2022 Feb 17. PMID: 35194352; PMCID: PMC8853293.*
9. *Gopalakrishnan, R. and Mogato, M. (2016). 'Bangladesh Bank official's computer was hacked to carry out $81 million heist', Reuters, 19 May.*
10. *Varadhan, S. (2018) 'India bank hack "similar" to $81 million Bangladesh central bank heist', Reuters, 19 February.*
11. *Paulus, S. (2018) 'Hacker greifen erneut Zahlungsverkehrsystem von Swift an', DerTreasurer, 19 February.*
12. *Jadhav, K. D. (2023). The Role of Cyber Security Audits in Managing Company Systems and Applications. Retrieved from: https://www.researchgate.net/publication/367559332*
13. *Verizon (2024) Data Breach Investigations Report.*
14. *Mohammed, D., (2015). Cybersecurity compliance in the financial sector. Journal of Internet Banking and Commerce, 20(1), pp.1-11.*
15. *Carter, W.A. and Zheng, D.E., (2015). The evolution of cybersecurity requirements for the US financial industry. USA: Center for Strategic and International Studies.*
16. *Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A. and Vrontis, D., (2021). Internal auditing and cyber security: audit role and procedural contribution. International Journal of Managerial and Financial Accounting, 13(1), pp.25-47.*
17. *Li, Y. and Xu, L., (2021). Cybersecurity investments in a two-echelon supply chain with third-party risk propagation. International Journal of Production Research, 59(4), pp.1216-1238.*
18. *Bhutta, M.N.M., Bhattia, S., Alojail, M.A., Nisar, K., Cao, Y., Chaudhry, S.A. and Sun, Z., (2022). Towards Secure IoT-Based Payments by Extension of Payment Card Industry Data Security Standard (PCI DSS). Wireless Communications and Mobile Computing, 2022(1), p.9942270.*
19. *Oluomachi, E., Ahmed, A., Ahmed, W. and Samson, E., (2024). Assessing The Effectiveness Of Current Cybersecurity Regulations And Policies In The US. arXiv preprint arXiv:2404.11473.*