World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Evaluating the role of cybersecurity audits in protecting the US capital market

Taiwo Paul Onyekwuluje [1], Daniel Akoto-Bamfo [2], Clement Tetteh Kpakpa [3], Benjamin Panful [4] and Derrick Oware [5,*]

[1] *University of West Georgia, GA, U.S.A.*
[2] *Temple University, PA, USA.*
[3] *Fox School of Business, Temple University, PA, USA.*
[4] *Department of Technology, Illinois State University.*
[5] *Department of Computer Science, Kwame Nkrumah University of Science and Technology.*

World Journal of Advanced Research and Reviews, 2025, 25(02), 974-980

Publication history: Received on 08 December 2024; revised on 23 January 2025; accepted on 26 January 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.2.0183

Abstract

More recently, the United States capital market has experienced a rise in cyber threats which pose an alarming threat to capital market stability and investors' confidence. This research explores how cybersecurity audits address these challenges. It highlights how audit committees have gradually started to consider cybersecurity as an important issue due to emerging threats. The Securities and Exchange Commission (SEC) has responded by adopting strict guidelines that insist that firms disclose their cybersecurity risk management policies and cyber incidents which emphasize the importance of accountability and transparency in the financial market (PWC, 2023). In addition, internal audit functions remain more critical today in evaluating the adequacy of cybersecurity risk controls, identifying vulnerability, and safeguarding sensitive information. Findings indicate that investors now consider cybersecurity disclosures while investing. Firms with no prior cyber incidents tend to gain from voluntary assurances, but companies with a history of cyber incidents face intense scrutiny about the competence of their management. Hence, this article emphasizes the critical contribution of cybersecurity audits in the protection of the US capital market by advocating for comprehensive risk evaluations, compliance with regulatory requirements, and proactive internal audit activities, thereby reinforcing the necessity of continuous improvement in cybersecurity protocols to maintain investor confidence and trust.

Keywords: Capital market; Risk management; Cybersecurity audits; Exchange Commission

1. Introduction

In the rapidly developing and closely linked financial industry, cybersecurity has emerged as a critical factor in protecting the reliability of capital markets. The U.S. capital market, one of the pillars of the world economy, relies on secure exchange of large amounts of financial information, critical for investors' trust and economic stability. However, as the financial sector becomes more digitalized, it becomes more vulnerable to cyber risks. Security breaches from data theft and infrastructure attacks in financial systems pose the risk of negatively impacting market stability, eroding trust, and leading to severe financial losses to institutions and individuals [1]. Hence, strengthening cybersecurity in capital markets is not just a matter of operational need, it is a public imperative that demands a coordinated approach of strict compliance with cybersecurity audits. Despite the financial sector's keenness on safeguarding its systems, capital markets have become one of the most attractive targets for cybercriminals. The capital markets have suffered sophisticated instances of hacking, phishing, ransom attacks, and data breaches which have intensified with the increased adoption of digital finance [2]. These threats are often targeted at the key infrastructures in the capital market, aimed at organizations that perform high-value operations and manage highly sensitive data. Recently, the U.S. Securities and Exchange Commission (SEC) and other regulatory organizations have noted the growing and more complex risk of cyber threats, urging the improvement of cybersecurity amongst financial institutions [3]. The fallout

* Corresponding author: Derrick Oware.

from just one major attack could severely undermine investor confidence and negatively affect financial flow, and in the worst case, catalyze economic instability.

In order to mitigate such risks, cybersecurity audits are shifting to become a central strategy of the capital market. These audits are established to assess the security posture of the institutions, outline areas of risks, enforce compliance and recommend actionable insights to institutions on how to improve their defenses. The value of cybersecurity audits lies in its capacity to reveal and mitigate vulnerabilities that might not be detected by traditional cybersecurity measures, acting as an extra layer of security against evolving cyber risks [4]. While security measures are one-time exercises that assess the strength of an organization's security solutions, security audits are recurring evaluations that review organization's conformity to the best practices and regulatory standards. Cybersecurity audits support capital markets with a proactive approach to threat prevention and resilience-building by facilitating an in-depth examination of security controls and protocols. However, the efficiency of cybersecurity audits in the capital markets has been criticized, particularly due to the increasing dynamism and sophistication of threats. One of such critics is the ability of audits to adapt with emergent cyber threats that require not only technological flexibility but also regular updates in laws and regulations. For example, most capital market firms face resource constraints and legal burdens as barriers to the adoption of comprehensive cybersecurity audits [5]. Also, the efficiency of these audits often hinges on the availability of standard metrics and benchmarks that can reliably measure the organization's security resilience and offer corrective measures for improvement. Despite the evolving awareness of audit as a critical component of cybersecurity compliance, the lack of uniform standards and guidelines for evaluating audit effectiveness can lead to variability in audit outcomes across firms [6]. Therefore, there is a need for further study on how cybersecurity audits may be refined to provide consistent safeguards across various entities within the capital market. This paper evaluates cybersecurity audit practices in the U.S. capital markets by examining current audit methodologies, barriers to implementation and the regulatory landscape. The contribution of this research will shed light on the role that cybersecurity audits play in informing future discussions over the best practices of audit implementation and the need to have standardized metrics in auditing evaluations in the financial industry.

1.1. Cybersecurity in Capital Markets

The capital markets have increased in operational efficiencies due to the introduction of digital systems, but this has also made it vulnerable to cyber threats. Cybersecurity has emerged as a major concern as capital markets, which mainly involve large-scale transactions and sensitive financial data are primary targets for cybercriminals. Researchers have recorded various cyber-attacks identified within the capital market, ranging from denial-of-service attacks and ransomware incidents to sophisticated phishing attacks targeted to steal sensitive information [7]. High-profile incidents like the breaching of major trading platforms and data theft of financial institutions highlight the vulnerabilities inherent in these systems [2]. If exploited, these vulnerabilities have the ability to create instabilities in the capital markets and not only individual firms, further risking broader economic repercussions.

A major vulnerability lies in the interconnectedness of capital markets, where various players in capital markets are dependent on common infrastructures and data flows. Growing reliance on third-party contractors and cloud services has introduced more complexities and risks that can be challenging to effectively monitor. According to Hain and Lindgaard, 2020 [8], capital markets are uniquely susceptible because of their constant rate of innovation in the development of new technologies, which often outstrips regulatory updates. Attacks stemming from the developments of these new technologies within the capital markets pose a risk to the core business of individual transactions, threaten integrity, and undermine investor confidence and the perception of security within financial domain. Therefore, it has become rather critical for capital markets to implement and enhance proper cybersecurity measures that suit their requirements.

1.2. Cybersecurity Audits

Audit committees are strategically positioned within organizations to ensure robust cyber security defenses, not in comprehending the minutia of the technology involved but by leading governance and policies [9]. Cybersecurity audits are structured assessments of an organization's security policies, procedures and infrastructure which are targeted at identifying vulnerabilities to establish compliance and regulatory standards. In the perspective of financial institutions, these audits play a dual role. They give an evaluation of security controls and also ensure compliance to regulations aimed at safeguarding the confidential client data as well as maintaining stability of the market [10]. Cybersecurity audits of institutions in capital markets may consider an institution's infrastructure such as firewall configurations, access controls, incidence response to security breaches, and compliance with cybersecurity standards among others. Studies show the importance of carrying out cybersecurity audits as a part of a proactive strategy to manage security threats. By having regular audits, financial institutions are able to identify probable security risks that could be exploited and implement corrective measures that will strengthen their security against cyber threats. Rosati et al., [11] note that

in addition to identifying current risks, audits offer actionable insights on improvement strategies that can be implemented in order to enhance cybersecurity planning over the long term. In addition, audits act as a policing instrument requiring firms to demonstrate compliance with various standards to be accountable to the regulatory bodies. In such competitive and sensitive environments like capital markets, where a single crack in security can have many widespread consequences, cybersecurity audits have turned out to be a standard measure of effective safeguard against risk.

While audits play a critical role in improving security in capital markets, these audits may vary in effectiveness depending on the scope of the audit, the approaches, the tools used, and the number of resources available. A critical concern is the absence of appropriate metrics and benchmarks for the assessment of audit performance. Lack of standard procedures hampers a rational comparison of the effectiveness of audits between different institutions, leading to inconsistencies in results among various firms. According to Rosati et al. [11], these audits are useful for determining compliance gaps but are not effective for evaluating the ability of an institution to respond to threats in real time, something that is essential to cybersecurity in capital markets. Another issue that is associated with comprehensive audits is that they can be very time and resource consuming and may be beyond the capabilities of small institutions in particular to undertake. Therefore, despite the need for audits, there is plenty of room to improve their functionalities and credibility. Deloitte's Center for Audit Quality recently conducted a survey that shows that cybersecurity is considered a major priority for audit committees with 69% respondents identifying it as a primary concern for the upcoming year [12]. This increasing emphasis is partly due to new regulatory requirements from the SEC that mandates companies to disclose their cyber risk and security incidents. More notably, 58% of audit committee members reported they have primary oversight over cybersecurity, which demonstrates a new shift in corporate regulatory practices to tackle the latest threats in the digital landscape.

1.3. Regulatory Background

An important source of influence on cybersecurity in the US capital markets is the regulatory landscape. The SEC issued the Regulation Systems Compliance and Integrity (Reg SCI) to set the standards for system integrity, security and resiliency among the technology infrastructure in the U.S. securities markets. The rules apply to entities that are important to the securities markets and could impact the market, investors, or individual securities. These entities include national securities exchanges, clearing agencies, alternative trading systems, and securities information processors [3]. Reg SCI requires firms to implement and apply policies for system monitoring, incidents response and disaster recovery to minimize the impacts of cyber-attacks. In its annual reports and guidelines, The Financial Industry Regulatory Authority (FINRA), a private American corporation that acts as a self-regulatory organization that regulates member brokerage firms and exchange markets, has also discussed the importance of cybersecurity, providing firms with measures on how best to protect clients' information from data breaches. In its recent report on cybersecurity practices in 2021, FINRA stated that for financial market security, areas such as data management, personnel identification, and event handling are essential [13]. It is for these reasons that cybersecurity assessments and enhancements must be ongoing, and audits as the primary compliance tool are crucial. Nevertheless, there are still some ongoing challenges regarding the non-uniformity of security standards across the industry. The SEC and FINRA guidelines provide a holistic framework but do not prescribe specific methods on how the purpose of these guidelines can be achieved. It remains the duty of every firm to decide which strategies are appropriate for the achievement of the regulatory standards. This flexibility may result in differences in quality and stringency of security procedures between various entities, which proves that cybersecurity audits are a necessity since they help in enforcing uniformity in the application of highly effective security practices. As cyber risks keep evolving, the regulatory authorities may be required to revise their guidelines and codes of practice to cope with the rising complexity of threats in capital markets.

1.4. Analysis of Cybersecurity Audits in Capital Markets

In 2024, the analysis of current practices for capital market firms on cybersecurity audit show some improvements from the previous because of the awareness on cybers risks and investors' confidence. Deloitte's Center for Audit Quality recent survey highlights how cybersecurity has emerged as the top priority for audit committees, with 69% of respondents indicating it as a primary concern for the upcoming year and an increase in increase from previous years. In the survey, 58% of audit committees reported having primary oversight over cybersecurity risks, indicating a shift towards more proactive governance in this area [12]. Goldman Sachs has developed a comprehensive cybersecurity risk management system, which integrates the usage of several layers of defense. According to their Client Security Statement, the firm employs a risk governance model comprising three lines of defense. The first is The Information Security and Cybersecurity Program (ISCP) which is overseen by the Chief Information Security Officer (CISO). The next is the Risk and Compliance Divisions, which offer independent oversight and finally the Internal Audit function which offers independent evaluation over the control environment. This structured approach helps Goldman Sachs to recognize cybersecurity threats, estimate their risks, and manage them appropriately to meet all the existing regulatory

requirements [14]. The firm also always performs internal and external risk assessment that includes penetration tests and "red team" engagements to evaluate their security stance against potential breaches. They use these assessments to help inform the program initiatives and define where their controls need to be enhanced in terms of cybersecurity. Likewise, cybersecurity audits are included as one of the key operation strategies in JPMorgan Chase. After a massive data breach in 2014, the firm has set up a cybersecurity audit group that routinely evaluates the company's systems. This team works closely with external auditors to ensure that JPMorgan's security protocols are adequate and current. The firm's commitment to performance improvement in its operations is seen in its ongoing investment of advanced technologies and increased awareness of cyber-risk among employees through training [15]. By promoting awareness, JPMorgan aims to ensure that the organization minimizes the risk posed by human error which is a leading cause of security breaches.

Additionally, as part of its risk management, Bank of America has included creating and effective cybersecurity framework which includes cybersecurity audits as part of its annual audits in its quest to create a security-focused organization. The bank emphasizes the importance of training programs designed to create staff awareness as according to one analysis, phishing attempts increased by 61% in 2022 over 2021 [16]. This proactive approach goes beyond improving internal security but ensures that all employees are equipped to identify and respond to potential threats. In prioritizing training with the cybersecurity audit, the Bank of America seeks to create a more resilient organization in terms of cybersecurity. Charles Schwab has also adopted a robust cybersecurity framework that involves regular audits of its policies and practices. Their formation of the Risk Committee that reports directly to the board underlines the high value placed on operational risks including cybersecurity at the highest levels of governance. It is the role of this committee to ensure that cyber security is a priority in the organization, facilitating ongoing oversight and accountability for implementing risk management strategies effectively [17]. In their 2023 report, Wells Fargo explains how their Board's Risk Committee has a primary oversight responsibility for information security risks and is responsible for the approval of the company's information security programs which include data protection and cyber resilience. The Board's Risk Committee has primary oversight responsibility for information security risk and approves the Company's information security program, which includes information protection and cyber resiliency. The Risk Committee receives regular reports from the company's Head of Technology and from Operational Risk Management representatives on their information security risks, and the Board receives a report from the Head of Technology on Wells Fargo's information security program and receives reports from management on significant information security developments, including certain incidents involving third parties. The presence of these dedicated separate teams for periodic cybersecurity updates implies the compliance of the bank with its own internal rules and, simultaneously, with third parties [18]. This approach preserves the security of Wells Fargo and at the same time mitigates risks within its systems.

1.5. Case Studies

LockBit ransomware was launched on Dublin-based application software provider, ION Investment Group on 1 February 2023. The cybercriminal group LockBit gained access to the company's data, encrypted it, and then requested for monetary payment to release the data. They also threatened to release the stolen confidential data to the public if the money was not paid within a certain period. This cyber-attack significantly affected ION's derivatives platform which is a tool utilized by many banks, brokerages, and hedge funds. The attackers managed to shut down this critical tool for many financial institutions and indirectly cause a major disruption to their businesses. Customers could not complete the processes of their transactions which had a financial impact on ION, EU, and US trading operations. ION engaged its clients in a bid to restore the functionality of the platform. Business entities that had been involved in derivative trading had to develop alternative strategies by which they could conduct their business, which had an absolute effect on the financial markets. Even though the US Treasury asserted that the attack offered no systemic threat to the financial sector, this incident highlights the critical importance of comprehensive cybersecurity audits across the industry [19]. For this reason, corporations need to undertake extensive due diligence regarding third-party contractors, evaluate their cybersecurity capabilities, and negotiate and sign contracts and agreements that clearly outline security obligations and responsibilities. They must also constantly assess and audit these third-party practices to ensure their compliance with cybersecurity policies. ION is now on a mission to reinvent the operations of its business through the use of automation technology. According to its website, this implies 'improved decision-making, increased efficiency including cyber resilience, simplified complex processes and workforce empowerment".

Additionally, Capital One Bank in March 2019, suffered a significant data breach that leaked the details of about 100 million people in the United States and around 6 million in Canada. This breach was attributed to a former employee of Amazon Web Services (AWS) who exploited a firewall that was misconfigured to gain unauthorized access to Capital One's cloud storage. After the incident, Capital One conducted a comprehensive internal audit into its cybersecurity practices which disclosed discrepancies in its security protocols and cloud configurations. Following the results of this

audit, Capital One employed several measures to improve its security posture including investing heavily in cybersecurity and incorporating the learnings from this incident to further strengthen their cyber defenses and comprehensive cybersecurity audit processes [20].

These case studies highlight the critical differences in cybersecurity audit and their relevance in addressing cyber risks in capital markets. ION's incident emphasizes the necessity of continuous monitoring, third-party evaluations, as well as the integration of the automation tools, aligning with the NIST Framework recommendation regarding continuous monitoring [21]. This approach recognizes that an interval-based auditing model is inadequate in a constantly evolving threat environment, especially for systems that are complexly interdependent like capital markets with third parties. In Capital One's case, however, we can see the value of broad, traditional audits in identifying specific weaknesses, but it also highlights the limitations of relying on periodic evaluations. Capital One's audit focused on internal configurations and highlighted the need for cloud-specific security enhancements, which resulted in a more targeted response to strengthen and improve internal controls. The two cases show the varying effectiveness of cybersecurity audits depending on the frequency, scope, and integration of automated tools. Continuous monitoring and automation are revealed as key components in improving audit practices and presenting a more adaptive strategy to the volatile threat environment.

2. Discussion

The findings of this research provide a nuanced understanding of how cybersecurity audits shape and maintain the resilience of the American capital markets in light of emerging cyber threats. Cyber incidents as evidenced by cases such as ION Investment Group and Capital One show that there exist significant blind spots audit practices from third-party risk management to cloud risks. These cases highlight that while audits have historically provided valuable compliance insights, they are now at a crossroads. The nature of the current infrastructure of financial markets requires dynamism, constant evolution, and the introduction of AI-driven practices, which are crucial for the sophistication of current digital infrastructure in the financial markets.

Market participants and regulatory authorities are required to shift from compliance-focused practices to resilient, anticipatory approaches due to the evolving landscape of cybersecurity in capital markets. The success of future audit practices depends on the right balance between compliance with regulations and adaptive, real-time security insights provided by AI tools. Automation allows firms to monitor data access patterns and flag any irregularities that otherwise may not be recognizable by human scrutiny or until the next interval-based audit. For instance, if ION had detected data access anomalies earlier, then LockBit's ransomware encryption may have been preempted or at least minimized in the scope of its impact [22].

Moreover, as firms move towards continuous monitoring, audit practices can focus on response readiness and managing crises – a shift from compliance to operational resilience. This change in focus may motivate firms to develop more robust incident response plans that are tested and refined through consistent audit exercises. When integrated with artificial intelligence these audits can simulate potential breaches and provide valuable insights into an organization's readiness in real world scenarios. The transition from a reactive to a proactive stance on cybersecurity, based on continuous audit-driven insights and recommendations, not only improves individual organizational security, but also strengthens the overall resilience of the capital markets, by providing early identification of the vulnerabilities among sectors.

This analysis supports and builds upon previous studies that have pinpointed primary gaps in general cybersecurity audits within financial markets. The findings of this research aligns with prior findings that underscored the importance of more automated and continuous auditing procedures. However, the specificity of the capital market in this study adds to the ongoing conversation on how interconnected systems and third-party dependencies intensify risk. Where prior research mainly focused on analyzing audit practices in silos, this research emphasizes the compound risks unique to capital markets and calls for audit frameworks that address third parties and cloud reliance comprehensively.

2.1. Future Directions for Research and Policy

Going forward, future research should explore frameworks for integrating AI-driven continuous monitoring with regulatory audit standards, providing firms with the ability to fulfill compliance while dynamically adapting to emerging threats. Research might also examine the economic and operational feasibility of mandating continuous audits across diverse financial institutions, assessing cost-benefit impacts on both large and small entities. Additionally, studies that investigate how capital market firms can optimize internal governance structures to accommodate these evolving audit practices would offer valuable guidance on fostering a culture of cybersecurity resilience. In future research, the evident

focus should explore frameworks for integrating AI-based continuous monitoring and regulatory audit standards in order to equip firms with the capacities of continuous compliance while dynamically adapting to emerging threats. Future studies might also look at the economic and operational practicality of mandating continuing audits across different financial institutions with an assessment of relative cost-benefit effects on large and small institutions. Further, studies to understand how capital market firms can optimize internal governance to support these rapid changes in audit practices would also provide valuable insights for building a cybersecurity culture of resilience.

3. Conclusion

This study reveals that cybersecurity audits in U.S capital markets require more than just traditional compliance checks and must consider more proactive AI-driven practices that address the complexities of today's rapidly evolving threat landscape. Examining recent events, this paper shows that interval-based auditing fails to capture key vulnerabilities in security, given the capital markets' increasing reliance on third parties and cloud infrastructure. Continuous monitoring and automation appear to be not only simple upgrades but as essential changes needed to protect interconnected financial systems. Regulatory bodies can contribute a decisive role in the level of enhancement of market-wide resilience by setting standards that support change, embracing technology, and adapting to it. At the same time, firms need to prioritize a security culture that goes beyond regulatory requirements, along with embracing a proactive security model and response. These new developments in audit practices are not only going to strengthen the stability of individual institutions but also make the broader financial ecosystem stronger, secure, and resilient in an age of accelerating digital transformation.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Wang, H. E., Wang, Q. E., & Wu, W. (2022) 'Short selling surrounding data breach announcements', Finance Research Letters, 47, 102690.

[2] GUMA, ALI & Mijwil, Maad & Buruga, Bosco & Abotaleb, Mostafa. (2024). A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech. Iraqi Journal for Computer Science and Mathematics. 5. 10.52866/ijcsm.2024.05.03.004.

[3] SEC (2023) SEC Proposes to Expand and Update Regulation SCI. Available at: https://www.sec.gov/newsroom/press-releases/2023-53

[4] Bozkus Kahyaoglu, S. and Caliyurt, K., (2018). Cyber security assurance process from the internal audit perspective. Managerial auditing journal, 33(4), pp.360-376.

[5] Reetz, M.A., Prunty, L.B., Mantych, G.S. and Hommel, D.J., (2017). Cyber risks: Evolving threats, emerging coverages, and ensuing case law. Penn St. L. Rev., 122, p.727.

[6] Didenko, A.N., (2020). Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond. Uniform Law Review, 25(1), pp.125-167.

[7] Tosun, O.K., 2021. Cyber-attacks and stock market activity. International Review of Financial Analysis, 76, p.101795.

[8] Hain, D.S. and Lindgaard Christensen, J. (2020), "Capital market penalties to radical and incremental innovation", European Journal of Innovation Management, Vol. 23 No. 2, pp. 291-313. https://doi.org/10.1108/EJIM-07-2018-0144

[9] CFO Journal (2024), "Cybersecurity and ERM Top Audit Committee Agendas". Available at: https://deloitte.wsj.com/cfo/cybersecurity-and-erm-top-audit-committee-agendas-5f67bb08

[10] Haapamäki, E. and Sihvonen, J., (2022). Cybersecurity in accounting research. In Artificial Intelligence in Accounting (pp. 182-214). Routledge.

[11] Rosati, P., Gogolin, F. and Lynn, T., 2022. Cyber-security incidents and audit quality. European Accounting Review, 31(3), pp.701-728.

[12] Deloitte (2024) Audit Committee Practices Report: Common Threads Across Audit Committees. Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-audit-committee-practices-report-final-2024.pdf

[13] FINRA (2021) Report on FINRA's Examination and Risk Monitoring Program

[14] The Goldman Sachs Group, Inc. (2024) Quarterly Report on Form 10-Q for the Quarter Ended September 30, 2024. Available at: https://www.goldmansachs.com/investor-relations/financials/10q/2024/third-quarter-2024-10-q.pdf

[15] Petru-Cristian, Btc Negrea. (2023). A Comprehensive Analysis of High-Impact Cybersecurity Incidents: Case Studies and Implications. 10.13140/RG.2.2.17461.65763.

[16] Security Magazine (2022) 'Over 255M in phishing attacks in 2022 so far', Security Magazine, 26 October. Available at: https://www.securitymagazine.com/articles/98536-over-255m-phishing-attacks-in-2022-so-far

[17] Charles Schwab (2024) SCHWAB CHARLES CORP 10-K Cybersecurity GRC - 2024-02-23

[18] Wells Fargo (2024) 2024 Sustainability & Governance Report. Available at: https://www08.wellsfargomedia.com/assets/pdf/about/corporate-responsibility/sustainability-and-governance-report.pdf

[19] Huang K, Wang X, Wei W. and Madnick S. (2023) The Devastating Business Impacts of a Cyber Breach. Harvard Business Review. Available at: https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach

[20] Shaharyar Khan, Ilya Kabanov, Yunke Hua, and Stuart Madnick. (2022). A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned. ACM Trans. Priv. Secur. 26, 1, Article 3 (February 2023), 29 pages. https://doi.org/10.1145/3546068

[21] Dempsey K., Chawla N. S., Johnson A., Johnston R., Jones A. C., Orebaugh A., Scholl M., Stine K. (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930.

[22] (Robertson Harry, 2023) ION brings clients back online after ransomware attack – source Available at: https://www.reuters.com/technology/ion-starts-bring-clients-back-online-after-ransomware-attack-source-2023-02-07/#:~:text=Lockbit%20said%20last%20week%20a,market%20participants%20in%20derivatives%20markets.