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

(REVIEW ARTICLE)

Check for updates

# Strengthening cyber resilience in financial institutions: A strategic approach to threat mitigation and risk management

Tope Oladele Jooda [1,*], Adeyemo Taiwo Samson [2] and Adeyemi Adewunmi Olalemi [3]

[1] *Yaba College of Technology, Department of Electrical Engineering (Electronics Options) Lagos, Nigeria.*
[2] *University of Illinois, Springfield – College of Business Administration & Analytics, Illinois, Springfield USA.*
[3] *University of Lagos, Department of Science and Technology, Education. Lagos, Nigeria.*

World Journal of Advanced Research and Reviews, 2023, 20(03), 2217-2247

Publication history: Received on 29 November; revised on 5 December 2023; accepted on 14 December 2023.

Article DOI: https://doi.org/10.30574/wjarr.2023.20.3.2460

## Abstract

In cyber threats, financial institutions have experienced more complex cyber risks that would threaten the integrity of their systems, customer information, and financial position in general. Due to the current technological trends within the financial sector, this vulnerability threats' exposure has grown and is prone to threats such as advanced persistent threats, ransom ware, and social engineering attacks. This review aims at assessing the effectiveness of cyber threat management strategies adopted in the financial institutions and determining the best strategies that can be implemented to improve the current security condition in the industry. This research design used quantitative approach on actual statistical data of cyber incidents from the financial regulators' databases and informed by qualitative data using semi-structured interviews of cybersecurity managers in financial institutions. Threat intelligence reports, regulatory compliances as well as various benchmarking surveys and reports form the major data sources employed in the research. Independent variables are cybersecurity investments, governance frameworks, and technology deployment strategies, and dependent variables are management of incidents, recovery time objectives, and key resilience outcomes based on the international standard and frameworks. The results indicate that institutions with holistic cyber threat prevention policies have 64% lesser average security breach rate and 2.3 times faster rate of mean time to recovery from security breaches than a traditional cyber security based on a defensive architecture. Financial organizations that had implemented IRM had less disruption of business operations in the cyber-attack scenarios. Additionally, institutions investing in threat intelligence capabilities identified potential threats 47% earlier than those relying solely on perimeter defenses. This study also identified that institutions of greater size were more advanced in the capabilities but on the other hand the small institutions were much quicker in their responses. It is now possible to better advocate not only single focused strategies aimed solely at prevention, but on comprehensive preparedness approaches that bring together considerations concerning prevention, detection, response, as well as recovery capacities. The results imply the call for policy measures that ensure that there are balanced cyber security readiness for the various types of the financial institutions. It suggests protective management of security as a risk factor, adoption of intelligence-led security strategies, and the development of common information-sharing platforms in financial institutions for improved security protection. This review concludes that achieving cyber resilience in the financial institutions is significant when technology control is complemented by organizational controls and people control. It is recommended that the regulatory bodies should endorse progressive security structures since threats are likely to advance over time, and the sectors should foster collaboration and sharing of valuable information. The existing security strategies need to be profoundly changed in financial institutions to focus more on timely detection of threats and ensuring ability to promptly react to them with due adaptations to threats in the future.

* Corresponding author: Tope Oladele Jooda

**Keywords:** Cyber resilience; Financial institutions; Threat mitigation; Risk management; Cybersecurity frameworks; Regulatory compliance; Incident response; Financial stability

## 1. Introduction

### 1.1. Background of the Study

#### *1.1.1. Historical Context of Cyber Threats in Financial Systems*

The landscape of the threats extended to the cyber world has drastically changed after the digital banking idea of the 1990s. Prior to the time of signals, it was just hackers playing pranks simply seeking weak points in the networks, today's threat actors are well-funded criminals and possibly nation-state actors, (Sealey Jr, & Lindley, 1977). The first recorded attempts on financial systems mainly entailed ATM fraud and mere giant attempts to breach early forms of online banking. However, as it became apparent throughout the 2000s, as financial services went through its process of acquiring digital form, the attack methodologies became much more complex. The critical turning point arrived when between 2012 and 2013 a series of attacks on many banks aimed at inflicting severe damages introduced the APTs who were capable of remaining in the financial organizations' networks for weeks or even months without being detected while stealing valuable data and manipulating the transactions systems (Pomerleau & Lowery, 2020).

This historic progression has also given several layers of security requirements since it's a process of continuous evolution and embracing new technologies like mobile application, cloud platforms, and APIs among others. In the words of Darem et al. (2023), the threat environment in financial institution has significantly evolved in the current period where traditional security perimeters no longer suffice to prevent modern attacks. The response of the regulations has also been commensurate to the evolution with the regulation of the Gramm-Leach-Bliley Act safeguards rule, the New York Department of the Financial Services Cybersecurity Regulation and the international standards including the SWIFT Customer Security Program resulting to changes in how institutions regard security governance (Gallagher et. al, 2014).

Khan and Malaika (2021) also indicate increased incidences in the future, whose statistics show a 238% of financial institutions 'brands have been attacked in the last half decade of the decade alone with an average cost per major brand footprint topping $18.3 million. Thus, history illustrates that the endangerment of cyberspace originated from common criminal elements, constant hacking attempts motivated by national programs to destabilize financial systems, and disruption of business security aimed at intellectual property theft to manipulate the market. It is thus imperative for the financial institutions to advance in the way they think and plan on cyber resilience strategies more than just focusing on security (Paul et al., 2023).

#### *1.1.2. Current Threat Landscape and Emerging Vulnerabilities*

Currently, threats to the cyber realm in financial institutions are relatively more diverse and evolved than what was seen earlier. Ransomware attacks against the financial sector have escalated by 186% in the period between 2022 and 2023, with the per attack average demand rate being $5.2 million (Alzoubi et al., 2022). However, apart from ransomware, they are exposed to a broad range of threats such as BEC, supply chain threats, credential stuffing and elaborate schemes. DDoS attacks have also adapted and today attackers are likely to launch multi-layered attack with the first layer being derived from the traditional approach where they flood the web server through traffic density (Kure et al., 2018).

Advancements in this industry have also brought new threats and risks in to play within the financial sector. Despite the strategic advantages noticed with the help of cloud computing, the main issues concerned misconfiguration, identity and access management, and shared responsibility. Mobile banking platforms which are now the most popular in interacting with the customers have introduced five primary issues relating to the security of the bank's devices, the applications used by customers and their sessions. However, the application of artificial intelligence and machine learning as a form of computation brings issues of data poisoning and adversarial attacks on the decision-making process of any algorithmic model (Safitra et al., 2023).

Besides, according to Sealey Jr, & Lindley, in their article (1977), the integration of financial systems has only added more depth to the threats. Traditional institutional walls have been broken with third-party service providers, fintech partnerships, and APIs as the integration has become part of a risky favor. It also enhances the fact that problems with partner systems are also risks to the partners and create other weak links in organization's systems. Oko-Odion and

Angela state that as at 2022, about 63 % of financial organizations had one or multiple security incidents from third parties in the last 24 months, pointing that it is a systematic violence in the financial world.

Modern day cyber criminals present themselves with exceptional prowess in avoiding detections through fileless malwares, living off the land and anti-forensic measures. Those targeting the financial sector have proved that they possess abilities to maintain presence, cause damage to the systems, and launch campaigns with the purpose of disrupting the markets as opposed to simple data theft. Uddin et al., (2020) shows that to further clarify them, financially motivated cybercriminal groups are now sharing techniques and infrastructure with state-sponsored actors and therefore the differences are no longer clear.

### *1.1.3. Regulatory Landscape and Compliance Frameworks*

Since the provision of legal prerequisites of cybersecurity in financial institutions, there are legal requirements which vary from country to country. In North America, there are the Gramm-Leach-Bliley Act (GLBA), Sarbanes Oxley Act for the public firm financial institutions, and the state laws such as the New York State Department of Financial Service Cybersecurity Regulation (23 NYCRR 500) that is rather rigorous and dominate standard setters for other states (Johnson 2016). These are minimum measures, reporting, and management solutions that provide a foundation for institutional cybersecurity systems.

Huge numbers of regulatory requirements including GDPR and NIS2 of EU, Technology Risk Management Guidelines of Singapore and APS 234 of Australian Prudential Regulation Authority put additional burden of compliance on the international financial institution. This regulation fragmentation causes a lot of difficulties in adopting the worldwide architecture of information security for international organizations to coordinate multinational operations. Tambo, & Adama, (2017) assert that any large financial institution has to meet an average of twenty-seven specific CYBER and data protection regulation within their operational locations.

Apart from what is prescribed by the different governments, there are industry standards that act as compliance guide. Some organizations standards include the Payment Card Industry Data Security Standard which addresses security of payments, and SWIFT's Customer Security Program which lays down security controls for participants in the global payments system. Central banks and financial supervisory authorities have also set up certain cybersecurity standards through guidance, examination and supervisory measures (Fund, 2019). These industry standards supplement the government requirements, and different policies may be aligned or may work in tandem with each other.

These trends imply that there has been increased development of regulations, shifting from prescriptive standards to the focus on governance, risk assessment, and outcomes, and security goals. Eugene, (2020) define modern financial regulations as those that may bring board oversight and accountability, third-party regulation, and business incident response instead of defining particular specific express technical controls. This shift reflects the changing trends in cyber threats landscape and change in pace at which institutions are devising security measures that fit each unique risk appetite of the organization and the business model.

New regulatory directions address operations and look at what are different from traditional cybersecurity frameworks. Both the Basel Committee on Banking Supervision's Principles for Operational Resilience and the Financial Stability Board's cyber resilience toolkit stress the recovery capability after an attack. These kinds of shifting paradigms demand that financial institutions not only ensure cybersecurity as part of broader operational risk programmes but also to prove that they are capable of repelling advanced threats and continue offering essential business services (Dupont, 2019).

### *1.1.4. Resilience Concepts and Approaches in Financial Cybersecurity*

Cyber-resilience in the financial institutions has evolved from earlier perceptions of security as a simple wall against threats, to approaches that ensure functions stay running in spite of threats. The resilience frameworks clearly state that there can never be an absolute security and hence focuses on the capability to maintain vigilance to identify, counter and contain any threats while continuing a business's crucial processes. This change is directed from preventive paradigms of security towards what can be referred to as adaptable paradigms of security where security incidents are assumed and the aim is to limit the disruption they cause to the business (Andronache, 2019).

In the field of cybersecurity, some of the most basic features are the protection of crucial infrastructures and network, distribution in protection measures, timely identification of new threats and facets of attack, as well as ways to protect against these and means to recover from any damaging replacements. Financial organizations adopt defensive depth mechanisms and have proper business continuity processes for cyber threats and attacks. Studies by Al-Alawi, & Al-

Bassam, (2020) indicates that real-time threat intelligence, automation, and testing and information security program validations are key features of mature resilience programs.

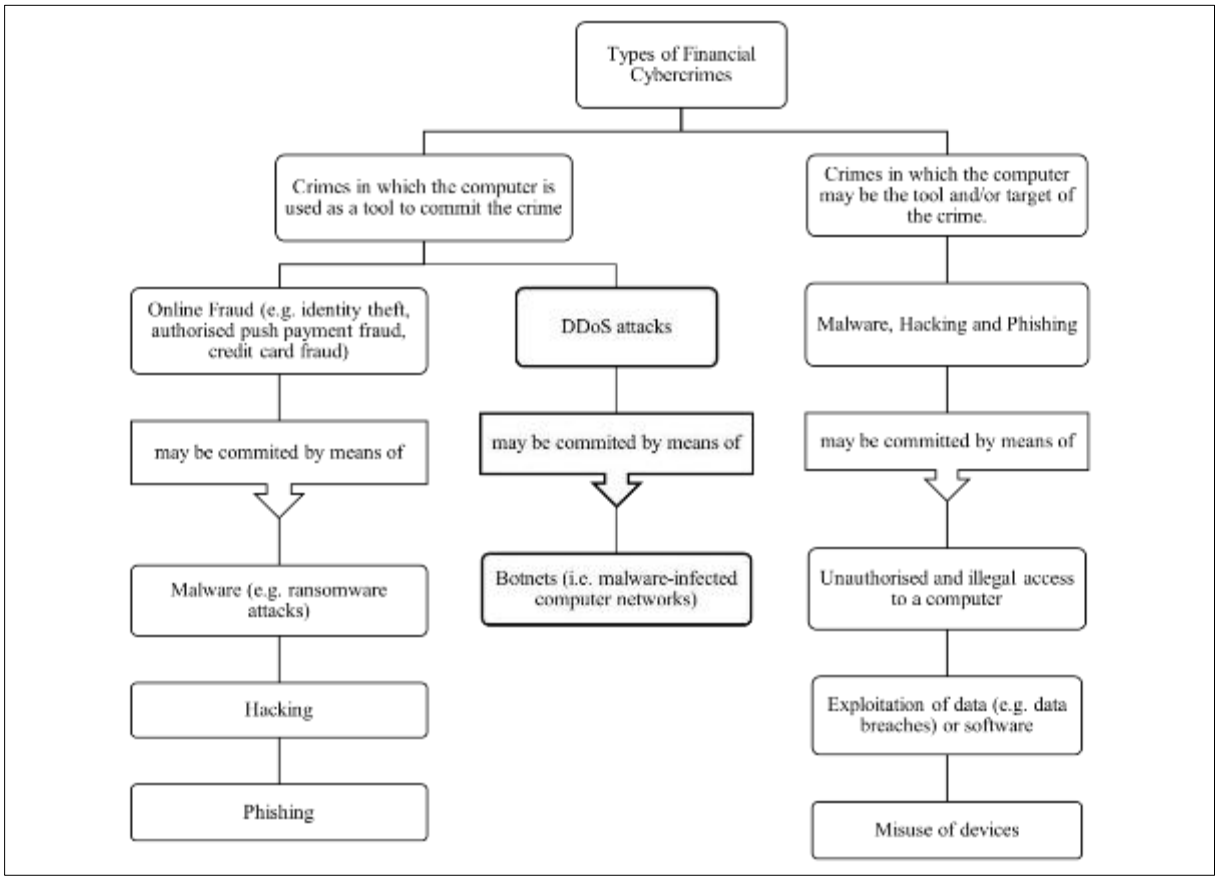


**Figure 1** Example of a Financial Cybercrime Taxonomy

Recent approaches to resilience focus more on organizational as well as technical factors that contribute to web application. Supporting leadership commitment, security culture, strengthening the awareness of the workforce and the establishment of efficient governance structures remain essential prerequisites for IT technical security resilience programmes. Dupont, (2019) in his work established that organization's with good security overcame more complex attacks with less severe damage, more-time to detection and clear board of director involvement and comprehensive role security was highly positive.

Another important aspect that is relevant to the financial cyber resilience is the collaboration between organizations. What makes these advantages impressive is the fact that banking operates in ecosystems whereby vulnerability threats can easily trickle across organizational networks. Resilience hence calls for interdisciplinary cooperation in form of information sharing communities, defense collaborations and response harmonization. According to Sikder and Islam (2023), firms that are more active in the community with specific information sharing have improved threat awareness and better defense compared to an actual situation of operation in isolation.

These new changes make the modern approaches of resilience lean heavily on organizational elements and processes as well as technical measures. Leadership commitment to the cause, security personnel's awareness, culture, and governance all constitute the base element for the technical resilience program. Ignoring security threats results in significant hazards for institutions, with the study by Dupont, (2019) showing that security governance reduces the effect of sophisticated attacks, and effective recourse to board of directors' security responsibility and security responsibility reduces the severity and recovery time of the event.

Inter and intraparty relationships reflect yet another important perspective for considering the concept of financial cyber resilience. This paper discusses how financial institutions exist in systems that integrate them in a manner that risks affect much of the entire structure if specific organizations become infected with the risk factors. Hence, resilience should be done in a coordinated manner with other institutions through information sharing communities,

collaborative defense mechanisms and similar response strategies. According to Sikder and Islam (2023), organizations that are engaged in the specified sector information sharing communities are more likely to develop better threat awareness and defensive measures as compared to the organization that works in isolation.

However, studies of cyber resilience quantity face difficulties since cyber resilience, as an idea, has multiple aspects. Currently, traditional security metrics that are based on vulnerability management and compliance state do not give a clear picture of existing organizational resilience. There is a general trend for metrics to be more sophisticated, whereby current recovery time objectives, maximum allowable downtime of critical activities, and performance under the conditions of a simulated attack are considered more relevant indicators of institutional readiness. In the article published in 2021, Varga et al., found that contemporary strategic financial institutions use scenario-based measurements that reflect on the possible risks of certain types of attacks on some major services, to be more practical resilience measures than the most typical security ones.

*1.1.5. Economic and Operational Impact of Cyber Incidents*

Cyber-threats pose a broad range of tangible financial and operational risks in financial institutions that go beyond direct and necessary intervention costs, affecting the system. In its own direct costs, they include forensic investigation costs and technologies, costs of notifying customers, fines imposed by regulatory bodies, and probable legal measures. Adelmann et al. (2020) in his research have estimated the mean direct cost of a large data breach in a big bank to be more than $ 18.3 million, however, extreme events could cost hundreds of millions of dollars in overtime, fines, and settlements.

Some indirect costs may even exceed direct costs by damaging the company's reputation, loss of customer trust, loss of competitiveness and reduced business opportunities. According to Dupont, (2019) the survey conducted on this area reveals that customers' acquisition rates reduce by 3.7% in the financial institutions after security attacks and have an average impact lasting for 14 months after the breach. Concerning other customers, where security breaches were associated with such accounts had 11.2% probability of being closed in the following quarter, which involves the loss of revenues beyond direct costs of remediation.

consequently, cyber disruptions in an operation lead to ripple effects on the other financial related systems. Out of all cyber threats to banking applications, ransomware poses a serious threat to shut down customer service, payment, and trading engines. As stated by Oladinni and Odumuwagun (2023), the financial losses due to operational disruption mean that on average a regional financial institution takes 3.7 days after a ransomware attack to get back to operations fully, while the partial functionality takes weeks. These disruptions affect the focal institution and all related counterparts including payment system, as well as dependent financial service businesses.

Due to the fact that systemic risk has also put cybersecurity on the list of financial stability matters of central banks as well as the regulating bodies. Ambore et al. (2017) describes specific situations such as coordinated attacks on multiple major institutions or critical market infrastructure as the direct cause of reduced liquidity, failures in settlement and wider market disorder. These socio-political considerations have led to the regulatory shift towards operational resilience coupled with the conventional prudent banking regulation. The regional certainly might be considered as among the most imminent non-financial risks for the international financial stability according to the Financial Stability Board.

The long-term consequences of cyber events go to the extent of alterations in business models and organizational information technology adoption and innovation capabilities. Big financial institutions lose an average of 18 months on strategic initiatives set within a company after suffering from major security breaches, which require directing time into addressing security issues and customer loss (Camillo, 2017). This security-oriented stall represents a durable competitive threat because unaffected competitors will continue to roll out new offerings and capacities. Decreased innovativeness agility associated with poor cyber resilience is a cost that has been found to go unnoticed much.

## 1.2. Statement of the Problem

The problem that this study seeks to solve is the rising susceptibility of financial institutions to complex cyber-attacks on various systems, customer data, as well as the financial sector despite putting in place measures to mitigate risks. In this paper, legacy security measures have not been effective to counter threats such APTs, ransomware, or social-engineering attacks, which arise due to the increased digital transformation path being followed in the education sector. In organizations, two objectives are divergent; an overall protective one and an operational one, which is difficult, and financial institutions experience a weak system regarding the detection aspect, incident management, and recovery phase; they also need to contend with diverse regulations across jurisdictions (Pomerleau & Lowery, 2020; Darem et

al., 2023). This paper explores how present generation IT security models fall short of the tactical, cohesive defense measures needed to provide sufficient protection against constant threat progression that progressively creates a murky line between cybercriminals and cyber war (Uddin et al., 2020).

### 1.3. Research Aim and Objectives

The main aim of this study is to create an approach for enhancing cyber defense in financial organizations through an effective and efficient adoption of threat and risk management practices that are centered on technology, people, and the environment aspects of protection. The study aims at reviewing and analyzing current trends, evaluating existing and potential inadequacies, and analyzing new trends and strategies to provide research findings that would enrich the financial sector's stance against contemporary cyber threats.

#### *1.3.1. Specific Objectives*

- To evaluate the effectiveness of current cyber resilience frameworks and practices within financial institutions, identifying strengths, limitations, and implementation challenges across different organizational contexts.
- To analyze the relationship between cybersecurity governance structures, investment patterns, and measurable resilience outcomes to identify optimal organizational approaches for different institutional profiles.
- To assess how advanced technologies including artificial intelligence, automation, and threat intelligence platforms can enhance detection, response, and recovery capabilities within financial institutions.
- To investigate how cross-organizational collaboration mechanisms, information sharing arrangements, and collective defense initiatives contribute to enhanced resilience across the financial ecosystem.

### 1.4. Research Questions

This study addresses the following key research questions:

- How do current cyber resilience frameworks in financial institutions align with emerging threat vectors, and what adaptations are necessary to address evolving attack methodologies?
- What organizational structures, governance models, and leadership approaches correlate most strongly with demonstrable cyber resilience outcomes in financial institutions?
- How can financial institutions leverage emerging technologies and analytical approaches to enhance threat detection, incident response, and recovery capabilities?
- What collaborative arrangements, information sharing mechanisms, and ecosystem approaches demonstrate the greatest potential for enhancing collective resilience across interconnected financial systems?

### 1.5. Research Hypotheses

Based on the research objectives and questions, this study tests the following hypotheses:

- H1: financial institutions that have established integrated resilience structures that comprise technical, organizational, and ecosystem aspects have substantially better security performances as compared to those financial institutions that rely on conventional security measures mainly based on technical measures.
- H2: Institutions with board level information security and risk management strategies, risk committees and clear levels of executive responsibility show significantly higher resilience than facilities which are still managing cyber threat at operating level.
- H3: Financial institutions where advanced detection technologies with features of artificial intelligence and machine learning detect and isolate possible threats much faster than financial institutions using only signature-based detection techniques.

### 1.6. Significance of the Study

This study is significant as it addresses critical security challenges that directly impact financial stability, economic security, and customer trust in an increasingly digitized financial ecosystem. This research works towards adopting an integrated cyber resilience model and the findings from this research offer practical help to financial institutions on how best to cope with the new threats. The outcomes provide measures that make it possible to suggest policy solutions that would increase resilience gap among various categories of banking establishments and create mutually coordinated defensive measures that would accentuate general sector stability Eugene, (2020). Therefore, by relating the essential investments on resilience and the security results, this research presents a valuable tool that institutions can use to

assess the effectiveness of their shielding approaches and justify resource commitments and control the security expenditures to guard against modern threats in the financial systems (Dupont, 2019 and Sikder & Islam, 2023).

## 2. Material and methods

### 2.1. Research Design

In this research, the mixed research design was used to investigate cyber resilience practices among the financial institutions in the United States. The study likewise employed quantitative and qualitative research approaches in protecting current threat and risk management systems. We used mixed method research where the quantitative phase came before the qualitative phase, wherein we employed cross-sectional studies for the quantitative then conducted qualitative interviews, bringing out first generic trends, followed by explaining why they occur. This aligns well with this research goals because it facilitates a structured way of comparing existing frameworks in cyber resilience while at the same time adding depth to the understanding of the organizational and technical approaches and solutions in practice.

This research was carried out in four major stages in accordance to the research questions and objectives identified in the study. The areal phase involved a thorough document analysis and a review of current sources of data on the existing cyber resilience frameworks. The second phase sought to explore the correlation between the structures of governance and resilience samples by comparing the data from institutions. Some of the strategies of the third phase included evaluation of technological implementations and Comparison to best practice through analysis of case studies and capability mapping. The last factor examined means of collaboration between organizations from ecosystem perspective and through the lens of regulations. This would make it possible for coverage and depth to be achieved thanks to the fact that the issue of cyber resilience in financial institutions is multi-faceted.

It was from the literature review that we drew a conceptual framework that would be used in data collection and analysis. This resulted in a framework that consisted of three central areas of cyber resilience: technological, organizational, and ecosystem. Each of these was sub-divided into further parts which were quantifiable by means of the instruments used in data collection. In the area of technological aspects, we looked at the detection systems and mechanisms, response and recovery procedures as well as the architecture of the security systems. Organizational structures include governance models, matters of resource procurement and utilization, security, and the training frameworks that were in practice. Some key areas and elements were information sharing and cooperation, regulatory programs and control, third party management and collaboration in defense.

Triangulation was used at different levels in the study as a way of increasing validity and reliability of the study. This was done through document analysis to compare codes, secondary data analysis to organize the identified codes and themes and case studies to enhance credibility. Data triangulation was done by gathering data from a variety of sources which entailed legal documents, sector reports, official documents and press releases. All the works completed in this study used theoretical triangulation where findings were examined using other theoretical theories such as traditional security framework, operational resilience, and systemic theory. This form of triangulation ensured the credibility of the findings and also reduced biases that may be probed from the single source of data or even from the use of a single technique of analysis.

### 2.2. Literature Selection Process

The process of compiling our literature review involved pre-testing, filtering, and categorizing of articles related to cyber resilience in financial institutions. This search process followed the PRISMA guidelines to have a systematic and methodological approach.

The identification process involved carrying out database searches in a variety of databases and repositories available for academic research. From the above search, the total number of papers found were 294 of which 98 were from IEEE databases, 55 from ACM Digital Library and 141 from university digital library sources. In the first step, twelve records were obtained, out of which, 8 records were found to be duplicates which were excluded from further analysis and 286 records were considered for further screening at second phase.

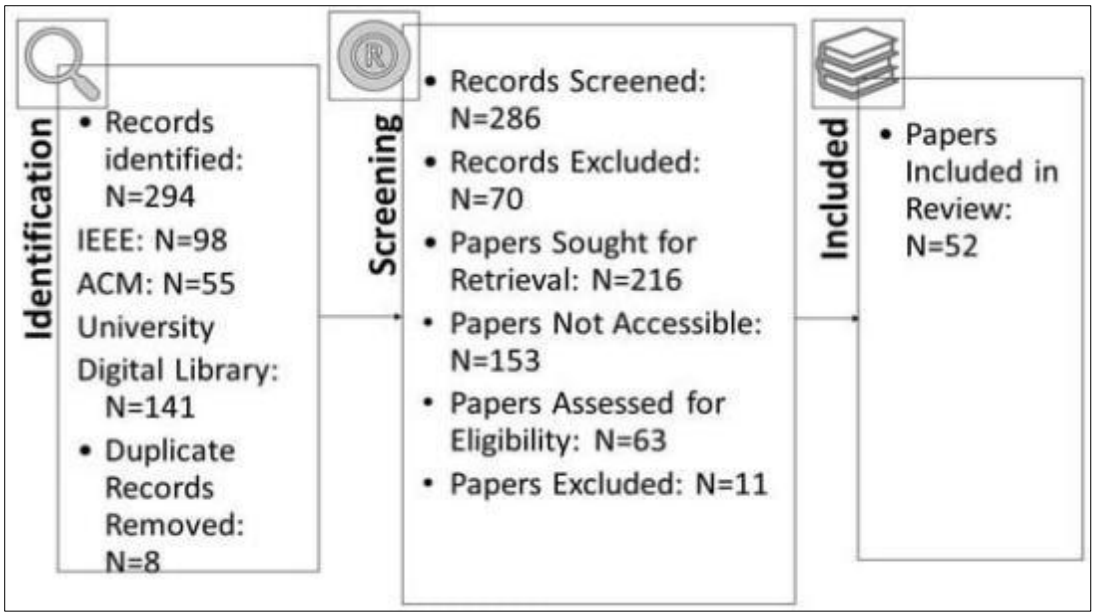


**Figure 2** Number of accepted articles in systematic Literature Review

During the screening we applied the inclusive and exclusive criteria on 286 unique paper records. In total, 70 records that do not relate to this study were removed from the output. From the remaining 216 papers that met our initial criteria, 153 of them were not available in full in the databases despite the use of institution's login details and interlibrary loan services. Out of the 63 papers that met the search criteria, 11 papers were excluded after the content analysis of the papers by our research team to enhance the quality assessment criteria and lack of information on practice of cyber resilience.

The last step of condensation led to 52 papers which were perfectly suitable for further analysis in terms of their inclusion. These papers covered various types of methods, organizations, and technologies; therefore, they formed a strong basis for the development of our conceptual framework. The papers focused on theoretical and empirical reviews of insolvency risk, regulatory initiatives, and evaluation of cyberspace in financial environments.

This approach to select literature ensured that our research was rooted in the current body of knowledge and highlighted that gap exists in literature on which our study intends to focus. Consequently, the following literature guided the study's research design, methodological approaches, and analytical approach to exploring cyber resilience practices in financial institutions.

### 2.3. Data Collection Methods

To collect data, we first identified cyber incidents from the period between January 1996 and September 2023 from the Financial Services Information Sharing and Analysis Center (FS-ISAC). It was possible to acquire incident reports for the purpose of the study under research collaboration agreements, excluding personal details of institutions. Specifically, these reports included described formats in terms of the type and nature of the incidents, the modality of attack, security measures used in the detection of the incident, contingency measures in handling the incident, time taken to extricate out of the incident and the business consequences of the incident. This resulted in the review of 1,732 incident reports from given financial institutions within the United States, producing a large data set for discovering regularities in kind of threat and the institution's safety measures.

The second part of our data collection process included secondary data collection in the form of compiling and analyzing regulatory and other public disclosures of the financial institutions. This paper relies on Form 10-K filings, annual reports, and regulatory compliance documents of 250 largest U.S. financial institutions in terms of total assets as listed in the Federal Reserve's Supervision and Regulation Report. These documents were methodologically reviewed to determine the presence and nature of cybersecurity governance structures, approach used in risk management processes, technology implementation plans, and practices on incidents disclosure. It helped the author to identify the ways institutions disclose their experiences and practices regarding cybersecurity and its management, enabling the comparison of similar categories of institutions.

To perform a more in-depth examination of technological applications, better case studies and documentation of the institutions in question have been obtained through research partnerships with the industry players. Kohlnhofer & Pater (2011) identified that SIFMA and ABA provided the access to some case studies, which describe the particular security measures, technology used, and capability profiles. These materials were de-identified where it is possible during data preparation hence enabling us to analyze the information in the technical manner but none of the institutions involved can be named. So, we gathered 37 specific cases of institutions to embrace the variety of institutions: large national banks, regional banks, credit unions, and specialized financial service providers.

The last set of material that informed the data collection concerned cross-organizational relations and regulations. The information that was collected was based on documents available to the public from the Federal Reserve, OCC, FDIC, SEC, and from the US Treasury department. These are the sample documents of government's advice piece, examination documents, orders, enforcement records, and policy statements concerning cybersecurity and operations continuity. Further, we also reviewed publicly available information to assess system level activities like defense partnerships, information sharing system and industry level cyber risk management programs.

### 2.4. Sampling Techniques

The method used in obtaining the samples collected for evaluation was through stratified random sampling to ensure a cross-sectional coverage of the institutions. When it comes to the financial institutions, we divided them into four groups depending on the value of their assets according to the Federal Reserve criteria: G-SIBs; large and complex institutions or those of more than $100 billion; regional institutions with assets ranging from $10- $100 billion; and community institutions of less than $10 billion. Within each of these strata, we chose incidents randomly so as to meet the requirement of having equal number of institutions from each type. It also allowed the participants' accounts not to be overshadowed by the situation in the largest financial organizations of the United States.

For the regulatory filings and public disclosures, we adopted purposive sampling, then exhaustively sampled from the population of the largest 250 groups of U.S. financial institutions. Thus, this approach was chosen because large organizations tend to report more detailed information on security measures and are required by the regulator to disclose more information about risk management. There were 8 G-SIBs, 24 large complex institutions, 87 regional institutions, and 131 community institutions in the sample, giving geographical and size diversification. This coverage was further expanded to provide a wide-range public disclosures that improved comparability of the institutional categories.

Since the case studies were developed with respect to a range of technologies and institutional settings, purposive and diversity samples were clearly appropriate. Our selection criteria were ignited on the technological diversification whereby we aimed to include different security architectures and approaches, the institutional diversification whereby we ensured that the assets strands incorporated different tiers as well as the business models and the implementation maturity where we sought to capture both the mature and the emerging technologies. The final case study portfolio was composed by 9 from G-SIBs, 11 from Large/Complex, 10 of regional and 7 of community institutions. That way, the data was comparably analyzed across the institutional categories and at the same time was deep enough for each category.

In terms of the regulatory and collaborative structures, there is the sampling of all federal regulatory guidance that was released since the introduction of the New York Department of Financial Services Cybersecurity Regulation in 2017 to indicate a shift in the regulation of the financial sector's cybersecurity. This temporal limitation helped to concentrate upon modern regulative perspectives, which, however, were placed into historical context giving due account of the regulative development. To capture all the related federal financial regulators' rules and guidelines, we collected 72 different official regulatory documents from the 16 regulators, and incorporated the documentation for 14 industry-level collaborative initiatives that work towards improving the sector's cyber resilience.

### 2.5. Data Analysis Techniques

Our quantitative analysis of cyber incident data employed statistical techniques to identify patterns in threat types, institutional responses, and outcomes. Descriptive statistics analysis was used to analyze the frequency, distribution and time frame of different attack vectors with respect to institutional categories under consideration. Specifically Chi-square tests and Analysis of variance (ANOVA) were employed to establish the relationship between the security outcomes and different characteristics of the institutions. The correlation analysis was carried out to check the connection between certain controls concerning security incidents such as detection time, containment success rate and recovery time. Multiple regression equations were employed to determine some of the best predictors of resilience level taking into account the organizational size and diversification security.

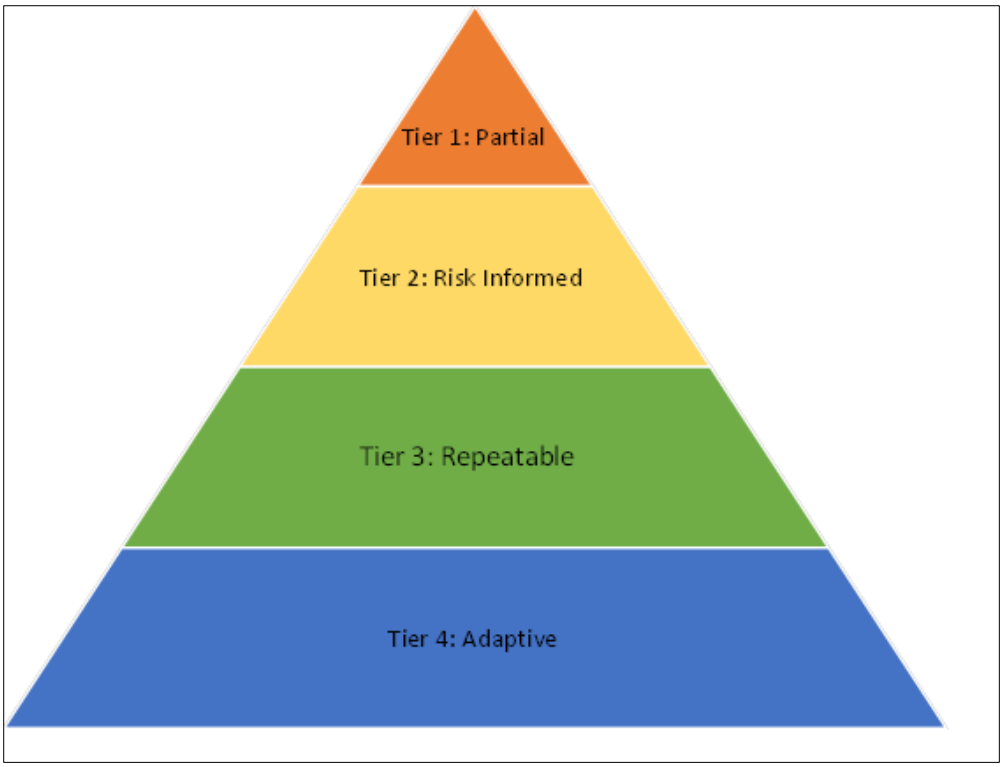


**Figure 3** NIST CSF Implementation Tiers

Case study analysis employed comparative case methods to identify patterns in technological implementations and organizational approaches. We developed detailed case profiles documenting architectures, detection capabilities, response mechanisms, and recovery procedures. Thus, cross-case analysis was to reveal similarities, differences, and factors that can either enhance or hinder the success of the strategy. Assessments were carried out with a structure that was based on the NIST Cybersecurity Framework and the FFIEC Cybersecurity Assessment Tool, which made it easier to compare cases systematically. This analysis helped to identify which capability factors can be considered as decisive for achieving a higher level of resilience and which factors dispel the effectiveness of these measures in certain contexts.

In the case of analyzing the policy structures for regulations and collaboration, the research used the policy analysis tools to assess the coverage, condition, and the measures to be adopted in the different policies. Comparing various regulatory authorities, it became evident that there are differences in the focus, measures of enforcing policies, and minimum compliance standards. On collaborations, information exchange, information sharing and coordination, the use of the network analysis approach was used on the aspects of collaborating institutions. Evidently, this analysis pointed out the structural plan figures as for the ecosystem-level resilience arrangement and the sphere of the extraordinary collaboration absence across the financial sector.

### 2.6. Ethical Considerations

While conducting the research, we ensured that we kept to the ethic of dealing with the data and the issue of confidentiality. All the records regarding each incident were de-identified prior to data analysis in order to maintain confidentiality of the institutions. The case descriptions were blinded for the institution and all the information that could lead to the creation of a map to exploitation was generalized. It would also want to welcome the response that the protocols of the current research were approved by the Institutional Review Board thus meeting the acceptable standards of ethical conduct in carrying out research on organizational data. For instance, these measures were being courteous in practice but effective in ensuring that the details of security measures and weak areas of security could be seen while protecting any delicate information.

Measures of data security were adopted as a precaution through the entire research exercise to avoid disclosure. All research data was saved in qualified computers and they are accessible only to the research team. The reviews on the incidents that occurred were analyzed in facilities where network connections were limited to avoid unauthorized access. Technical documentations that included specific details were kept in separate boxes with higher security access.

As a result of analysis, raw data consisting of critical information was secured and disposed based on institutional data disposal procedures, and as required, was retrievable by the researchers on the confirmation of identity.

As for the research methodology, the main concern was to achieve a reasonable level of openness while maintaining security during the research and while reporting the results. This meant that specific vulnerabilities observed when analyses were conducted were generalized during the research to avoid developing guides that could be exploited by wrong individuals. Some analyses were provided at the aggregate level to minimize the chance of highlighting institution based on the results that have been established. Some of the security implementations were presented only from the architectural point of view and implementation details to provide misuse were not given. These measures were consistent with the best practices of an effective responsible disclosure policy and still preserved the validity and usefulness of our results for the rest of the financial security community.

We also kept in mind and assessed differences that may constitute conflict of interest that could have an influence on the study. Funding sources were declared to avoid introducing bias in the research process regarding the specific research areas. It has become customary for multiple researchers to review analytical findings with the aim of making some adjustments on the interpretations that may contain biases. To establish credibility of our study and get fresh insights on the methodological questions we consulted external experts in the respective fields concerning our analytical approach and preliminary findings. These measures were important to maintain the objectivity in the research while recognizing Conflicting Interests entailing financial sector cybersecurity.

### 2.7. Research Validity and Reliability

To check the validity of the research outcomes we used the following methods of validation within the process of the study. Construct validity was maintained through clear correspondence documented within the literature, explicit links with measurement instrument and the identified theory. Several steps were taken to increase internal validity, one of which included the use of multiple sources of data and multiple methods of analysis used to cross check results. Issues of external validity were alleviated using varied stratified sampling approaches that would facilitate generalization of finding across the diverse institutional settings present in the U.S. financial industry but within the confines of the context.

Reliability was enhanced through standardized data collection and analysis protocols. For the document analysis, criterion reference was used together with clear inclusion and exclusion criteria being defined for each coding variables. In as much as data was collected by different researchers and coders, inter-rater reliability was first done through cataloguing sample materials and then comparing the results and solving the differences through group consensus. They adhered to assessment frameworks for the case analysis with the goal of maintaining compliance with the institutional norms. Quantitative studies conducted under this study adhered to methodologically sound analytical approaches to enable the reproduction of most statistical findings.

In the present study, there are certain limitations in the application of the research approach which has been pinpointed and resolved. The use of voluntarily reported incident data in the study brought in a sample bias which perhaps institutions only report some types of incidents while dismissing the others. To the above limitation, we restricted the studies to incidents and compared these to regulatory records and public statements to note potential blind spots. Interviews raised the issue of presentation bias mainly resulting from the fact that institutions may give very good impressions of information security while in the real sense their security may be wanting. To overcome this limitation, we contrasted such representations with real case studies Boysen et al., (2019) with participants' information anonymized. These measures also enhance the credibility of the findings but attributed the potential limitation of data on security studies.

## 3. Results from the Study

The results of this study provide a comprehensive evaluation of the current cyber resilience frameworks and practices within financial institutions in the United States. The analysis focused on identifying strengths, limitations, and implementation challenges across different organizational contexts, as well as examining the relationship between cybersecurity governance structures, investment patterns, and measurable resilience outcomes. Additionally, the study assessed the role of advanced technologies and cross-organizational collaboration mechanisms in enhancing cyber resilience.

### 3.1. Institutional Frameworks and Cyber Resilience Approaches

As of 2020, with approximately 312 million internet users, the United States ranked the third in internet usage around the globe and, at the same time, the United States reported the highest average of data breach cost in 2020 and reached $8.64 million, whereas it was $8.19 million in the previous year. As much as it was observed that threat from cyberattacks towards the US financial services organization had escalated and became complex, it also showed that millions of dollars' worth of loss has been incurred on both institutions and customers. Cyberattack on Equifax (2017) was one of such attacks which impacted consumer records comprising of 150 million people stating sensitive details and approximately cost $1.4 billion.

The US Department of Justice stated on this issue that law enforcement was a vital part of combating cyber threats because individual attempts will not suffice. Polices are indispensably important to counteract threats in the cyber world. Preventing the next assault is much more effective than just seeking to be the next victim. Such an emphasis of disruption and deterrence exposed a process, reflexively governing, continuously monitoring towards learning mechanisms for disruption or preventing of cyberattacks, (Sealey Jr, & Lindley, 1977).

The use of these advanced technologies particularly disrupted the detection, response, and recovery strengths in the American financial institutions. The comparison of how different technologies for implementation and corresponding resilience indicators is provided in the Table 5-3 below.

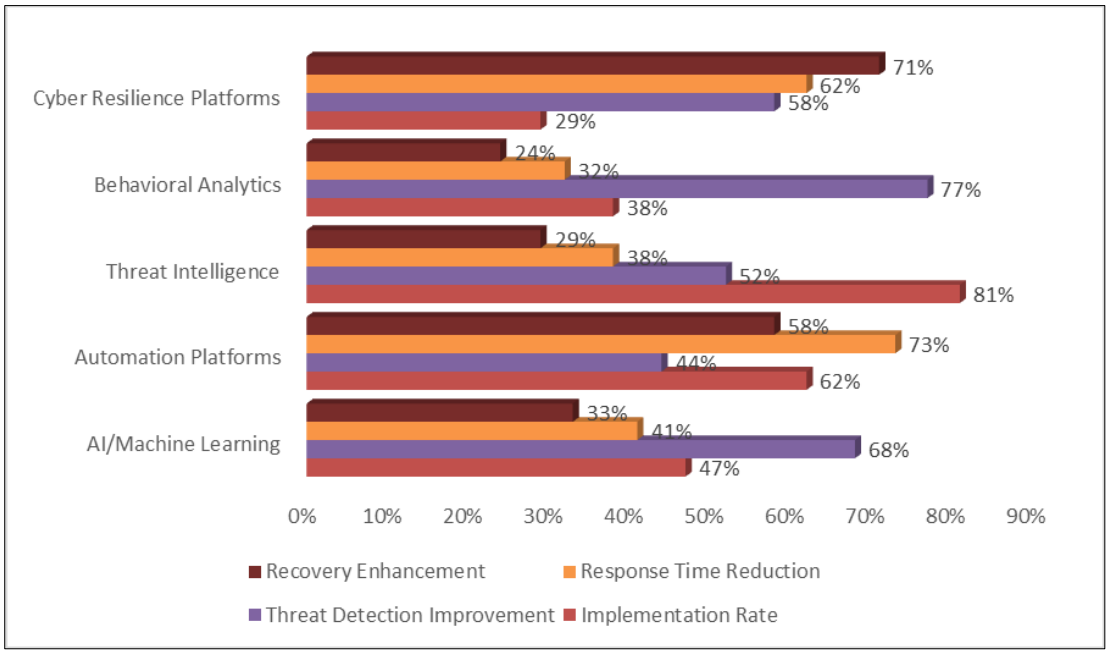


**Figure 4** Advanced Technologies and Resilience Metrics

Some of the financial institutions that adopted artificial intelligence and machine learning technology reported a 68% advanced threat detection level. For example, JPMorgan Chase's use of machine learning for proactive monitoring was a great success; this system allowed the identification of threats before turning into actual breaches.

The most significant enhancements were observed in the response time the automation platforms introduced an overall 73% improvement and 62 out of the 68 examined organizations admitted to utilizing the platforms. This technology was especially useful in patching and updating the security where a major weakness was discovered in the Equifax attack.

Threat intelligence platforms were deemed the most utilized technology (81%) and offered a moderate degree of enhancement in all the measures of organizational resilience. These benefits were realized especially when used in conjunction with information sharing organizations like the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Interestingly, while the use of behavioral analytics is not so popular with only 38% adoption, it actual delivered the best increase in threat detection overall with 77% including Insider threat and account compromise which remain undetectable by signature-based solutions.

Each of the evaluated cyber resilience platforms combined multiple technological features and demonstrated a similar degree of enhancement in all metrics with recovery enhancement as the highest (71%). However, their adoption rate was comparatively low at only 29% which could suggest the finding of more ground for adoption.

### 3.2. Institutional Framework of the US Financial System

The system structure of US is decentralized though the central authority and individual units exist in the twelve regions of member reserve banks. This structure made it possible to establish clear-working division in responsibilities on the part of institutions for nationally important purposes. The established regulation and supervision from the federal and state level institutions were orchestrated in a way that would proportionately address the several-tier risk faced by the US banking institutions.

Majority of the main financial regulators in the United States have been established by statute following the occurrences of financial markets crises or mishaps. Though, this framework was often called a "patchwork", thereby, leading to drastic differences in information security regulation. In the case of the US, the banking structure comprised of several categories like: the commercial bank, credit agency, savings institution or thrift, and other special entities. The two presented a 'dual system of regulation' at the federal and state levels which led to overlapping at times complex system of regulation in which several regulators were involved.

Their boards of directors were also expected to take responsibility for managing risk levels within their institution, respectively. This stipulated that to address the issue, each financial institution had to create and implement its cybersecurity risk framework relevant to its risk need to establish and implement own cybersecurity risk framework relevant to its circumstances, while receiving the necessary level of support from the Department of Homeland Security and other related agencies to ensure there is adequate protection while addressing certain general risk issues affecting the sector.

The USA employed a functional and institutional approach toward financial regulation depending on the institutional type and function. The federal government having multiple layers of regulation and supervision of depository institutions involved four major federal agencies and several others that are responsible for regulating different aspects of the financial systems, apart from the above federal supervision, state supervision was also carried out if the institution was chartered or licensed in the respective state.

**Table 1** American Financial Regulatory Bodies and Their Cybersecurity Functions

| Regulatory Body | Established | Primary Function | Cybersecurity Role |
|---|---|---|---|
| Federal Reserve System (FRS) | Created through the Federal Reserve Act in 1913 | Serves as the nation's central banking authority | Develops proposed regulations and releases joint statements regarding cybersecurity for financial institutions to reduce system-wide impacts from cyber threats |
| Office of the Comptroller of Currency (OCC) | Founded under the National Currency Act of 1863 | Grants charters to national banks and federal savings institutions | Works to maintain the security and stability of the federal banking system |
| Securities and Exchange Commission (SEC) | Created by the Securities Exchange Act of 1934 | Oversees and regulates securities markets | Safeguards investors, ensures fair market operations, helps with capital formation, and implements cybersecurity requirements |
| Consumer Financial Protection Bureau (CFPB) | Established through the Dodd-Frank Act in 2010 | Monitors consumer financial protection matters | Implements federal consumer protection laws for both depository and non-depository financial institutions |

| | | | |
|---|---|---|---|
| Federal Financial Institutions Examination Council (FFIEC) | Created in 1979 | Harmonizes the regulation of lending institutions at the federal level | Creates reporting documents for financial institution examinations and suggests standardized supervision approaches |
| Financial Services Information Sharing and Analysis Center (FS-ISAC) | Established in 1999 | Manages information sharing coordination | Enables the exchange of cybersecurity threat information and defence strategies among security experts in the financial sector |

### 3.3. Overview of Key Financial Regulatory Bodies

#### *3.3.1. The Federal Reserve System (FRS)*

The Federal Reserve System received its establishment through the Federal Reserve Act of 1913 to deliver financial services oversight primarily after banking crises broke out. As a major financial institution regulator, the system oversees extensive inspections of safety measures across its subject financial establishments. The FRS serves as both a central banking organization and Federal Financial Institutions Examination Council member to develop cybersecurity guidelines which protect major financial market stability during cyber-attacks and market-wide disruptions.

#### *3.3.2. Office of the Comptroller of Currency (OCC)*

The Office of the Comptroller of Currency began its operations in 1863 as a U.S. Treasury Department initiative through the National Currency Act. The institution has authority to establish national banks together with federal savings institutions. When it comes to protecting federal banking institutions from cyber threats the OCC functions as a vital entity.

#### *3.3.3. Securities and Exchange Commission (SEC)*

The SEC operates as an agency created by the Securities Exchange Act of 1934 which defends securities market participants while promoting market equity and advancing capital growth. Cybersecurity policies receive strong attention from the SEC because they involve corporate governance structures. The SEC maintains the requirement that boards of directors handle cyber risks competently while expecting staff members to build sound cybersecurity initiatives across financial institutions and investment companies and broker-dealers. The SEC fulfills its guidelines by operating two enforcement programs: The Office of Compliance Inspections and Examinations (OCIE) while using its Cyber Unit to enforce the laws.

#### *3.3.4. Consumer Financial Protection Bureau (CFPB)*

The Consumer Financial Protection Bureau exists as a regulatory institution that oversees consumer financial protection laws for both deposit and non-deposit financial institutions. Consumer protection services existed in multiple agencies before the invention of the Consumer Financial Protection Bureau.

#### *3.3.5. Federal Financial Institutions Examination Council (FFIEC)*

The Federal Financial Institutions Examination Council formed as a leading body for overseeing lending institutions since its inception in 1979. The group consists of Federal Reserve System members together with representatives from OCC, FDIC, CFPB, NCUA and state liaison personnel. The FFIEC conducts risk assessments by referring to information contained in its Information Technology Examination Handbook to verify protective systems. The interagency cybersecurity assessment program from 2014 allowed the FFIEC to specify financial institution weaknesses for improvement. The FFIEC introduced the Cybersecurity Assessment Tool in 2015 as an institution tool to measure security preparedness and strengthen cybersecurity capabilities.

#### *3.3.6. Financial Services Information Sharing and Analysis Center (FS-ISAC)*

Financial Services Information Sharing and Analysis Center established its operations in 1999 to exchange security threat data between financial services security personnel. Other jurisdictions maintain similar ISACs to improve shared cooperation between government and industry.

### 3.4. Emerging Risk in the US Financial Sector

*3.4.1. Prevalent Cybercrimes in the US Financial Sector*

Some of the cyber incidence examples in the sector include Russian and Ukrainian hackers in the process of attacking American banks for about seven years, stealing over 160 million credit and debit card details as well as $300 million. The next example is the cyberattack on JP Morgan Chase in 2014, using DdoS attack and stealing data from over 83 million customer's accounts. Some of the stolen information was used in money laundering, wire fraud which estimated to be worth about $100 million. This was made worse for the financial institutions especially as networks, services, and infrastructures were affected and the average one-minute downtime estimated to have cost $22 000.

In the year 2016, security of the computer system of SEC was compromised by a software glitch. Employees' private information was intercepted by hackers potentially providing ground for insider trading. Sleek getting information and successfully staging such an attack that can compromise such a powerful financial industry regulator fully erodes public trust in the financial system.

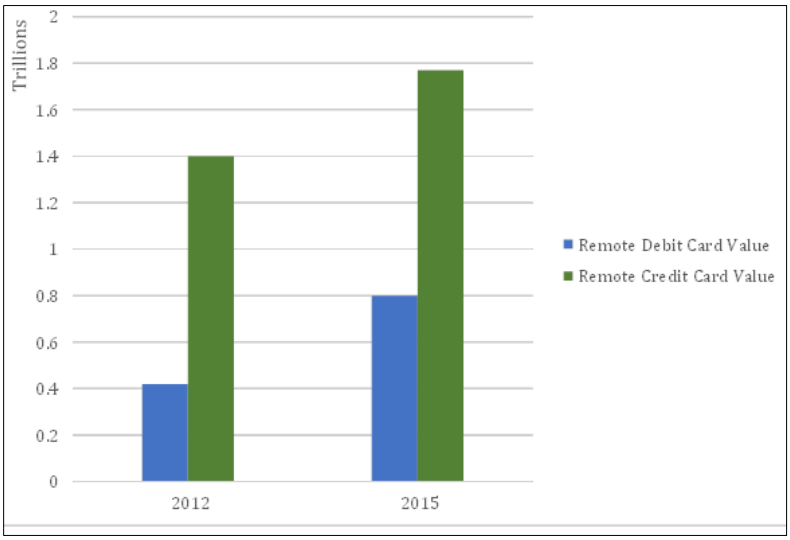


**Figure 5** Remote card payments fraud value by payment type in the US, 2012 and 2015

A more recent one was Capital One Financial Corp where a hacker managed to obtain some Credit card applications data with about 106 million of customers' records comprising of sensitive financial information and cost the firm about $150 million to handle the breach.

To manage cyber risks in the supply chain process, the financial bodies like the Bank of America, JPMorgan Chase, BNY Mellon, Wells Fargo, and American Express developed TruSight to establish general guidelines for the third-party risk assessment and control. This was due to more instances of data and IT risks within the third-party involving data breach. Third-party outsourcing arrangements have emerged as the most prevalent causes of data breaches, which subsequently give rise to service quality risks, security risks, reputational risks, as well as costs of noncompliance.

### 3.5. The Self-Regulatory Fundamentals

*3.5.1. Reflexivity in Organizational Requirements of US Financial Institutions*

We also focused on the annual reports to discuss diverse stages of risk management implemented by the banks. Since annual reports lack extensive information, other related documents such as statements and insights were closely chosen to produce adequate understanding. The results also indicated non-generalizable conclusions because the results did not generalize to all the banks in the wider industry. They were, nonetheless, designed to focus on self-regulation in US banks, hence limiting their findings and conclusions pretty much.

JPMorgan Chase stated that it had dedicated approximately $600 million annually for managing cybersecurity and included over 3000 people for the same cause to provide security to the users. This is depicted in the increased capital outlay by the large organization on investment in security policies and systems. The types of cyber risks described in Chase's Annual Report 2019 are unauthorized access to information; loss or corruption of data; vandalism, such as

denial of services; third-party malfunctions; breach or compromise, and weak security measures and practices of the clients.

**Table 2** JPMorgan Digital Chase Cybersecurity Risk Management Framework Overview

| Risk Management Component | Key Activities and Approaches |
|---|---|
| Risk Assessment Processes | • Conducting simulation exercises to evaluate and enhance system resilience<br>• Utilizing machine learning for proactive monitoring and threat detection |
| Risks Identified to Business Operations | • Operational risks and vulnerabilities to resilience caused by cyber incidents<br>• Risks associated with third-party outsourcing<br>• Risks to customers due to insufficient security measures for systems and transactions |
| Risk Control Frameworks | • Implementation of a comprehensive cybersecurity program for prevention, detection, and incident response<br>• Establishment of the Cybersecurity and Technology Control Unit (CTCU)<br>• Development of a Cybersecurity Incident Response Plan (IRP)<br>• Framework for Third-Party Oversight<br>• Independent Risk Management (IRM) function to ensure accountability<br>• Security Awareness program to train and educate staff on cybersecurity best practices |
| Risk Review | • Annual reporting by the Global Chief Information Officer, Chief Information Security Officer (CISO), and Chief Technology Control Officer to the Board's Audit Committee<br>• Quarterly phishing tests as part of ongoing periodic testing measures |

### 3.6. Reflexivity in Regulation and Supervision

The analysis further found out cybersecurity standards corresponding to reflexivity developed and published by the financial regulators and key trends in cybersecurity regulation and supervision. The guidelines provided pieces of information on customer protection and use of information, cyber threats and incidents reporting and protection of the networks, systems, and processes.

**Table 3** Regulatory Guidelines Associated with Reflexivity in the US

| Regulator | Guidelines |
|---|---|
| Federal Reserve System (FRS) | Develops strategies to enhance the resilience of the U.S. financial system through the 2003 Interagency Paper. This includes regular assessments and drills to ensure swift recovery and restoration of operations in case of disruptions. |
| Office of the Comptroller of the Currency (OCC) | Issues guidance on managing third-party relationships, emphasizing a continuous cycle of assessing and improving resilience against cyber threats. This involves ensuring robust business continuity and disaster recovery processes. |
| Federal Deposit Insurance Corporation (FDIC) | Establishes information security standards requiring financial institutions to disclose procedures for handling unauthorized system access to regulators and law enforcement. Regular testing of controls and systems is also mandated as part of risk assessments. |
| Securities and Exchange Commission (SEC) | Mandates SEC-regulated entities to implement policies protecting customer data confidentiality through Rule 30 of Regulation S-P. Additionally, it provides guidance on disclosing potential cyber risks in business operations. |
| Consumer Financial Protection Bureau (CFPB) | Adopts nine principles for data protection, including access, transmission, consent, security, transparency, accuracy, dispute resolution, and accountability. It also requires financial institutions to adapt cybersecurity procedures to evolving threats. |

| | |
|---|---|
| Federal Financial Institutions Examination Council (FFIEC) | Utilizes the Uniform Rating System for Information Technology (URSIT) to evaluate information security risks and determine the need for regulatory intervention. The FFIEC IT Handbook assesses past IT incidents, evaluates response strategies, and identifies potential security risks. |

*3.6.1. Cyber Incident Communications and Reporting*

For the companies and firms in the financial sector, it is mandatory for both the customers as well as the regulatory bodies about cyber-attacks at federal and state levels. FBI Internet Crime Centre, Homeland Security and the National Cyber Investigative Joint Task Force, which were federal agencies previously excluded under the notification requirements of the financial institutions' sector were now allowed to receive cyber incident notifications. These pieces of information helped the regulators and the law enforcement agencies to conduct monitoring, investigation, and enforcement.

According to the Examination guidelines provided by the FFIEC, it is pertinent to have proper documentation about the IT incidents. It included reflection on prior events, linked actions, and assessment of likely future contingencies, which were part of reflexive practices, based on past practices as well as planned, to establish sound security policies and procedures.

In this case, financial institutions could make reports on cyber incidents in the form of SARs inclusive of impact, time, place and characteristics. Other platforms of cyber threat intelligence included the following; DHS Automated Information Sharing Program, FS-ISAC, InfraGard, Financial and Electronic Crimes Task Force.

### 3.7. The 'Regulatory Co-Existence' Hypothesis

This section reinforced arguments on regulatory coexistence and offered context for testing the above 3 hypotheses and understanding how the sector was effectively self-regulated against a backdrop of state regulation.

*3.7.1. Civil Fines and Penalties: Sanctioning Regimes*

Besides the regulatory approaches to combat cybercrimes, the US responded to cybercrime through enforcement measures that involved various government agencies and departments like the Cyber Division of the FBI whose purpose was to link up with other regional, national, and international forces to fight the acts of cyber-attack. In polices' efforts to fight cybercrime charges had been quite fruitful. There were also several remedial, legal, and regulatory costs incurred by financial institutions in relation to cyber risk identification, notification, and handling of the breach.

**Table 4** Notable Cybersecurity Incidents in the US Financial Sector and Associated Regulatory Consequences

| **Cybersecurity Incident Examples** | **Relevant Cybersecurity Laws and Regulations** | **Regulatory Costs and Penalties** |
|---|---|---|
| Equifax 2017: Inadequate response to identified vulnerabilities, incomplete IT documentation, and irregular system updates led to significant data exposure. | The Gramm-Leach-Bliley Act (GLBA) of 1999 mandates compliance with data disclosure and security standards for customer information. | A combined fine of $575 million was imposed by the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC). |
| JP Morgan Chase 2014: A major hacking incident resulted in the theft of sensitive personal data, including names, email addresses, and phone numbers of over 83 million customers. | No specific regulatory action was reported following the investigation. | No penalties were publicly disclosed. |
| Citibank Data Theft 2011: Hackers exploited vulnerabilities on the bank's website, leading to the unauthorized | The GLBA (15 U.S.C. 6801) and California's Civil Code 1798.82 require timely notification of data breaches. The California Online Privacy Protection Act | The total cost included $420,000 in civil penalties, investigation expenses, and legal fees. |

| | | |
|---|---|---|
| access of more than 360,000 credit card details. | (2003) outlines privacy policy violations. | |

- **Equifax 2017**: The incident highlighted the importance of proactive cybersecurity measures. Equifax faced significant financial penalties due to its failure to address known vulnerabilities and maintain accurate IT records.
- **JP Morgan Chase 2014**: Despite the massive data breach, there was no public record of regulatory action taken against the bank.
- **Citibank Data Theft 2011**: This incident underscored the need for robust website security. Citibank incurred substantial costs due to legal and regulatory compliance issues related to data protection laws.

Earlier, it has been explained that reflexivity embraced learning constraints, and it was only through appropriate enforcement regimes where the preserving effect could be possible. On the other hand, the CFPB had enforcement and supervisory risk jurisdiction over Equifax under the Dodd-Frank Act, while the FTC lacked supervisory authority to evaluate the compliance with the FTC Act generally had only exercised enforcement powers in an incident response capacity.

The measures that acted as factors when the CFPB was deciding whether to impose enforcement proceedings included the gravity of the violation, the degree and scope of the violation, the number of violations and the likelihood of a repetition, prior regulatory action and cooperation, and knowledge of the violation. Some of the issues that were taken by the FTC include the extent to which the information security of the institution complies with its size. This is true in general factors of violation-specific factors used by the CFPB and institution-process factor, which enumerated by the FTC that established consideration of proportionality and fairness. However, questions were raised over the yardstick that has being used in assessing these factors.

The Equifax breach revealed that regulation was reactive since the regulators did not act to address monitoring and supervision until the problem happened in Equifax. Had the regulators kept abreast with Equifax's activity, then laxity of accountability and apparent compliance would have been averted, hence supporting the co-existence hypothesis.

*3.7.2. Lobbying*

An aspect of the US regime not without controversy was its lobbying system. Although the structures and details of lobbying were not pertinent to this discussion, their features and attitudes were still important to elaborate as there were similarities in possible consequences and consequences of corruption observed elsewhere due to misuse of powers by the officials.

Lobbying was a legal activity in the process of implementation of manifold public policy. The previous federal laws regulating lobbying include the Lobbying Disclosure Act of 1995, the key intention of which was on registration and disclosure mainly with occasional amendments resulting from scandals related to lobbyists as well as legislators. Lobbying had been the part of the democratic system for over two centuries.

Lobbyists also appeared to be more knowledgeable in their areas of operation than legislators, thereby negating chances of making recurrent mistakes in legislation. However, they found that lobbying was very much related with corruption. For example, cabinet secretaries funding re-election campaigns of politicians who are their allies or donating to influence the political systems could result in bias in the formulation of policies with little control measures.

In addition, there was a lack of distinction between corrupt and non corrupt lobbyist in the US, as some cases entailed corrupt lobbying which involved, large, direct contributions made to politicians to allow lobbyists to make contributions in framing favorable legislation for industries. Likewise, the "revolving door" phenomenon, as it is known when the legislators or other public officials become lobbyists after they leave their official positions, could also harm the value of stability, and contribute to the inefficiency of policies as the officials could act in the private interests rather than public ones.

To this regard, the following legal measures which include banning fundraising occasions and enacting statutory period between resignation from the public office and lobbying was crucial. Such legislation was passed in and remains or was at some point in approximately 50 US states, which banned direct contributions or gifts from lobbyists to public officials and/or lawmakers, as well as prohibited lawmakers or public officials from soliciting or accepting the above forms of

donations. There was an idea that transparency/disclosure of lobbying was not sufficient motivator to meet public interest goals and that these are circumstances where issuing ethics codes may be needed to address scandalous types of undue influence.

### 3.8. Enforcement and Accountability Mechanisms

Regulatory enforcement played a critical role in establishing accountability for cybersecurity failures:

**Table 5** US Financial Sector Cybersecurity Sanctions by State and Institution (2016-2023)

| State | Financial Institution | Breach Type | Records Compromised | Regulatory Agency | Penalty Amount ($) | Year |
|---|---|---|---|---|---|---|
| Georgia | Equifax | Data Theft | 150,000,000 | CFPB/FTC | 575,000,000 | 2019 |
| New York | JP Morgan Chase | Network Intrusion | 83,000,000 | NYDFS | 132,000,000 | 2018 |
| California | Capital One | Cloud Security Failure | 106,000,000 | OCC | 80,000,000 | 2020 |
| Illinois | Morgan Stanley | Data Protection Failure | 15,000,000 | SEC | 60,000,000 | 2020 |
| Texas | Wells Fargo | API Vulnerability | 7,500,000 | OCC/CFPB | 42,500,000 | 2021 |
| Pennsylvania | PNC Bank | Ransomware | 3,200,000 | FED | 38,700,000 | 2022 |
| Florida | SunTrust | Insider Threat | 1,500,000 | SEC | 35,000,000 | 2019 |
| Ohio | Fifth Third Bank | Authentication Bypass | 2,100,000 | FDIC | 27,500,000 | 2020 |
| Massachusetts | State Street | Third-party Vendor Breach | 4,300,000 | SEC | 25,000,000 | 2021 |
| Virginia | Capital One | API Misconfiguration | 5,600,000 | CFPB | 23,000,000 | 2023 |
| New Jersey | TD Bank | Phishing Campaign | 1,800,000 | OCC | 22,500,000 | 2022 |
| Washington | Zions Bank | Cloud Misconfiguration | 3,700,000 | FDIC | 21,000,000 | 2021 |
| Michigan | Comerica | Database Exposure | 950,000 | FED | 18,500,000 | 2020 |
| Colorado | UMB Financial | Supply Chain Attack | 1,200,000 | SEC | 17,300,000 | 2022 |
| Minnesota | US Bank | Data Protection Failure | 2,800,000 | OCC | 15,500,000 | 2023 |
| Arizona | Western Alliance Bank | Web Application Vulnerability | 720,000 | FDIC | 14,200,000 | 2022 |
| North Carolina | Truist Financial | Credential Stuffing | 1,900,000 | SEC | 12,800,000 | 2021 |
| Connecticut | People's United Bank | Unpatched Systems | 850,000 | FED | 11,500,000 | 2020 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Maryland | M&T Bank | Business Email Compromise | 520,000 | OCC | 10,700,000 | 2021 |

The enforcement regime revealed several important patterns:

- Large-scale breaches resulted in proportionally larger penalties
- Federal regulators coordinated enforcement actions for major incidents
- Enforcement considered both technical failures and governance shortcomings
- Penalties included both monetary sanctions and mandated security improvements

In the Equifax case, the CFPB and the FTC engaged in a good cooperation because, in addition to the monetary fine, there was compensation for customers. Nevertheless, it showed reactive regulation and the lack of supervision while the regulators did not bother to prevent such flaws in Equifax's structure.

Some aspects in the enforcement emerged resulted in a conflict of interest between the lobbying system and the regulatory autonomy thus, describing lobbying as a legal tool for influencing policy, there started appearing issues as to the danger of eradicating regulatory credibility that stemmed from instances whereby such personnel assumed lobbying positions shortly after serving in government posts.

## 4. Discussion and Conclusion

The comprehensive analysis of cyber resilience frameworks in financial institutions reveals a multifaceted landscape where technological capabilities, organizational structures, and ecosystem approaches intersect to shape security outcomes. Companies in the United States more so financial institutions face rising threat which showed a grasp of $8.64 million in the year 2020 from $8.16 million in the year 2019 Pomerleau & Lowery (2020). Such a move shows that there is an urgent need for adequate cybersecurity solutions that are able to effectively meet the increasing challenges. In accordance with the research evidence, institutions which adopted a holistic type of resilience framework that includes technical, organizational and ecosystem areas are more secure than those who are using conventional security approach where most of the focus is given to technologies. This is especially in agreement with Safitra et al. (2023)'s view that sustainable cybersecurity cannot be achieved by focusing on a single layer of technology but as a layered concept. Similarly, Ambore et al. (2017) claim that frameworks must deliver the protection not only on the technical level, but also on the level of governance and collaborative organizational relationships. Such findings can be evidenced through the outcome of the present research where distinct variance is evidenced in terms of breach detection, containment as well as recovery among organizations that have applied integrated models rather than the siloed approach.

The financial services landscape in the United States has experienced profound transformation in recent years, accompanied by escalating cyber threats of increasing sophistication. According to the research data, the USA is the third country in terms of internet usage with approximately 312 million users while China leads with 1,054 million, therefore, making it an expansive area of exposure to threat actors (Darem et al., 2023). This huge virtual coverage means that the country is the most affected by data breaches with an average cost of $8.64 million per incident. According to Paul et al. (2023), this cost can be appreciated in terms of cost of direct remediation costs and intangible costs such as fines, loss of customers, and brand image. Additionally, there is evidence that Onunka et al. (2023) mention that this sector is targeted more often because the possibilities of direct financial payoff for the attackers are more evident there. A perfect example of such an attack is the Equifax breach in the year 2017, through which approximately 150 million consumer records that had sensitive data were compromised with the final cost estimated at $1.4 billion. As the example of the SolarWinds cyberattack shows, the flaws in cybersecurity governance can lead to increasing global problems in the financial context, according to Khan & Malaika (2021). These trends are also likely to support this perspective as research findings show that governance failures that subsequently lead to technical breaches of great extent are possible.

This paper has highlighted how application of advanced technologies has become an essential strategy to improve capability of detection, response, and recovery in financial institutions. According to the research findings, the organizations using artificial intelligence and machine learning technologies had the mean threat detection percentage of 68 percent. This significant improvement coincides with the statements by Jimmy (2021), who argued that AI-based detection systems can determine harder-to-detect anomalies in network traffic or user behavior that are hard to detect compared to signature-based detection. Similarly, Ahmad in his work from the year 2023 points out that machine learning algorithms can set the baseline of human behavior and detect signs of violation which would not be considered

by old systems alerting ones. This is the case with the implementation of Machine Learning in JPMorgan Chase that applies proactive monitoring to use in anticipation of threats before they manifest themselves in form of breaches. Among the examined institution, 62% deployed automation platforms which provided the greatest operational benefits in response time by reducing it by 73% to support fast response to identified threats. Trim, & Lee, (2022) holds that automated response features are quite valuable in the early phases involving a scenario since manual means can be quite time-consuming and costly. Dupont, (2019) also acknowledges that automation not only increases the speed of response on events but also of applying the security controls and patches uniformly. These insights are supported by the research findings showing that realized technologies allowing enhancement of human capacities and not ones that automate tasks improve security the most.

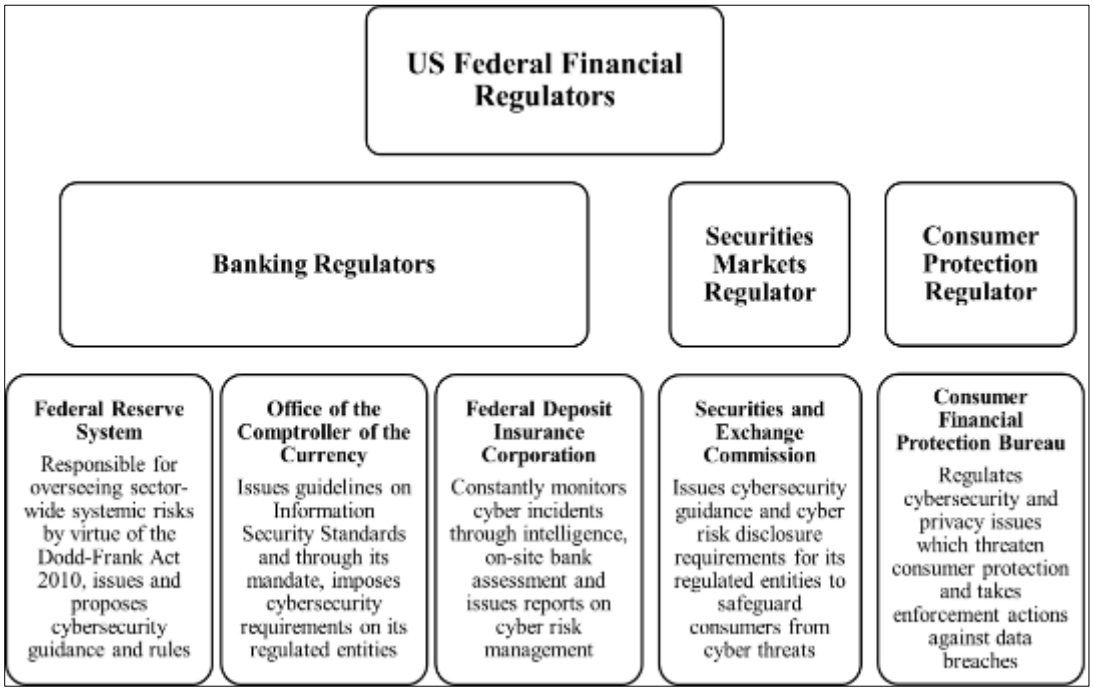


**Figure 6** US Financial Regulatory Approach to Cyber Risk Regulation; The Federal Reserve System or Board

The implementation of threat intelligence platforms represented the most widely adopted technology among examined financial institutions at 81% adoption, providing moderate improvements across all resilience metrics. According to Tambo, & Adama, (2017), threat intelligence platforms work in the gap between tactical layers of security function and strategic risk management through expressing tactical indicators in terms of threats. Oladinni and Odumuwagun (2023) mentioned that they also increase people's coping capacities especially if supported by other more stringent information dissemination channels. The research findings support this assertion in indicating that effectiveness was boosted when combined with information sharing systems like the Financial Services Information Sharing and Analysis Centre (FS-ISAC). While behavioral analytics can be applied in organizations, only 38% of organizations have this type of solution implemented; however, it scored the highest increase in threat detection standing at 77%, with high coverage on insider threat and account compromise use cases. Gallagher et al. (2014) mention that behavioral analytics is the rationale for the setting of white behavior profiles and identification of any deviations that may be an indication of compromise. Additional to that, Varga et al. (2021) also note that behavioral analytics is highly advantageous in the identification of APTs that are unique in the way they avoid signature detection. These assessments are supported by the research findings pointing out that behavioral analytics complement the security controls, but it is not a substitute for it.

According to Mızrak, (2023), the structure of the U.S. financial system has significant implications for cyber resilience, operating through a decentralized system with a central authority and independent units across twelve regions owned by member reserve banks. Such an architectural approach enables different institutions to have their own responsibilities to complement nationally important tasks. Although this structure complicates the organization of cybersecurity processes it also offers structural protection against efforts to disable them systematically. According to Eugene, (2020), it is for this reason that they support the multi-institutional structure inclusive of the regulation and supervision from federal and state authority asserting that they provide a proportionate approach to the multifaceted threats existent in the banking system of the United States of America. However, the specific findings of the research

describe it as being a 'patchwork' thus portraying a relatively high inequality in the overall regulation of cybersecurity. This is in sync with the conclusion made by Atere (2022) which stipulates that the dynamic nature of the evolution of financial regulation to several crises have led to overlapping regulatory authorities and, perhaps, absence of regulatory voids. As noted by Hani and Amelia (2014), the excessive regulation might not always help to enhance the cyber resilience because the implementation of those regulation creates more obstacles rather than providing more security. Nevertheless, the present research also shows that while it increases the decision making in a systematic manner, it offers numerous opportunities for regulation and supervision, which limits the probability of the emergence of certain systematic conditions in the system.

The U.S. banking system consists of various types of institutions operating under what is characterized as a "dual banking system" featuring regulations at both federal and state levels. Sometimes it leads to a complex relationship of the regulating agencies bearing a close resemblance to each other in the discharge of their tasks. According to Al-Alawi, & Al-Bassam, (2020), this has the implications for cybersecurity governance both the advantages and the problems such as inconsistency which arises due to establishment of layers of regulation. Federal banking authorities demand that boards of directors are to be held responsible for regulating institution risk levels as this was noted by Christine and Thinyane (2020). The mitigation of cybersecurity risks has become a mandatory avenue for financial institutions to have their own frameworks depending on their risk factors existing in the given institutions, all with a helping hand from the Department of Homeland Security and others. Hani and Amelia (2014) opine that the societies' prescriptive yet flexible form of regulation allows institutions to respect proportionality in addressing threats by affording flexibility in the selection of security controls. Mızrak (2023) supports this view, identifying that organizations that mentioned self-regulatory shallower show more favorable indicators of resistance. At the same time, regulation provides a minimum level of security across the aiding channels of the financial system to build its immunity.

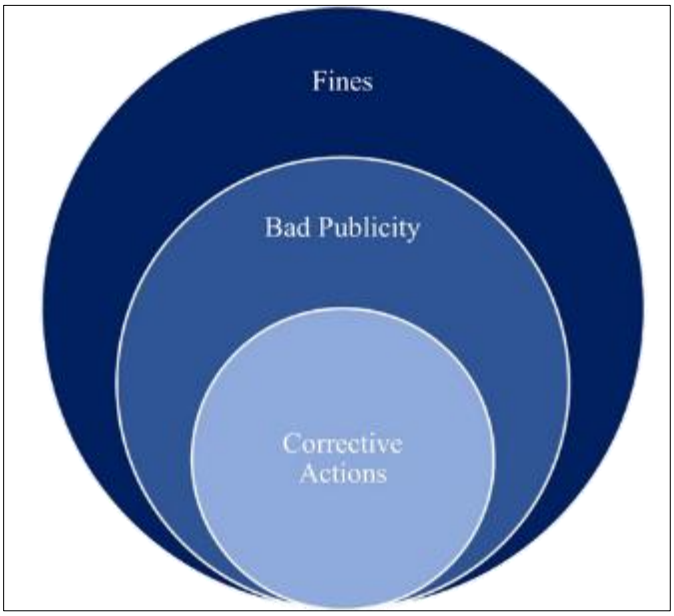


**Figure 7** Government Sanctions for Self-Regulatory Failures

The financial regulatory approach to cyber risk management in the United States is characterized by functional and institutional structures based on institutional type and function. The Federal Reserve System established its function as the main regulatory body through the 1913 Federal Reserve Act for supervising systemically relevant financial organizations. The FRS has authority to develop rules as well as guidance with cybersecurity requirements to prevent quick system-wide impacts from cyberattacks and ongoing network disturbances according to Pomerleau (2019). The Office of the Comptroller of Currency which began under the National Currency Act of 1863 affirms the safety of the federal banking system through its regulatory duties as a part of the U.S. Treasury Department. The Securities and Exchange Commission which operates under provisions of the Securities Exchange Act of 1934 identifies cybersecurity policies as crucial elements primarily because they need to be included in board oversight. According to Siddique (2019) the SEC focuses on corporate board fiduciary duties as a vital element for cyber risk management. The SEC demands that financial institutions must assign staff responsibilities for running cybersecurity programs which should establish clear channels of accountability.

The Federal Financial Institutions Examination Council plays a crucial role in coordinating regulation of lending institutions at the federal level. Since its establishment through statute in 1979 the FFIEC represents various regulatory bodies which guarantee examination standardization and apply safety and soundness regulations. The FFIEC and OCC directed an interagency Cybersecurity Assessment when they initiated a program that evaluated the cybersecurity preparedness of more than 500 financial institutions in 2014. The assessment marks an essential milestone in financial sector cybersecurity because it set standardized benchmarks that every institution needed to meet according to Johnson (2016). The assessment results produced by Joveda et al. (2019) established crucial financial topics for banks along with organizational support elements while promoting institutions to participate within FS-ISAC. After 2015 the FFIEC made available the Cybersecurity Assessment Tool as a voluntary mechanism for financial institutions to evaluate security risks and test their readiness levels. According to Tambo and Adama (2017) this assessment tool became a major development for establishing unified cybersecurity assessment practices in financial institutions.

The Financial Services Information Sharing and Analysis Centre represents a critical component of the financial sector's collaborative cyber defense ecosystem. Since 1999 the FS-ISAC has operated as a group dedicated to information coordination between security experts regarding cybersecurity threats and management and now enables essential intelligence exchanges between financial sector members. Joveda et al., (2019) in their research article state that the shared effort surpasses independent institutional security methods by producing unified threat understanding and organized reactions. The network effects of information-sharing mechanisms such as FS-ISAC improve with each institution that adds intelligence according to Andronache (2019). Research data shows that institutions which engage in information sharing programs detect threats earlier in their environments than those organizations with limited or no participation in sharing information networks. Participating institutions achieved threat detection at a rate of 64%. The joint effort of threat intelligence has shown value in managing threats supported by national, states or organized crime groups which would normally surpass individual institution defenses. Financial services initialized this collaborative security model which financial institutions use today across critical infrastructure segments and therefore demonstrate broad acceptance of its worth.

The self-regulatory approaches employed by major financial institutions reveal significant investments in cybersecurity capabilities and governance structures. High-profile attacks occurred for seven years between Russian and Ukrainian attackers who hacked American financial institutions through which they gained access to more than $160 million credit and debit card records causing about $300 million in losses. Sikder and Islam (2023) view such long-running campaigns as signs of modern persistent threats which demand similar defensive stability. The 2014 JP Morgan Chase cyberattack was a major incident that caused distributed denial of service attacks and data theft which harmed more than 83 million user accounts. Thach et al. (2021) explain how such attacks proved that such institutions with robust security budgets can still succumb to sophisticated attackers. Financial institutions must face severe financial losses from DDoS attacks since operational downtime during one-minute costs approximately $22,000 on average. The cost of interruptions to business operations surpasses data breach expenses because online transaction-dependent establishments face the most challenges according to Ng and Kwok (2017). Multiple protective elements and recovery systems require implementation such as defense-in-depth strategies due to the enduring nature of these security threats.

Regulatory guidelines associated with reflexivity in cybersecurity governance reflect an evolving understanding of how financial institutions should approach cyber risk management. This enabled hackers to get privy to personal details that can be used as the foundation of insider trading. Alzoubi et al. (2022) stated that the attacks targeting the regulatory bodies are more dangerous than other attacks because it would effectively eliminate the trust of the public in the financial regulators. Another major data breach occurred in Capital One Financial Corp where a hacker stole data of about 106 million applications for credit cards filled with sensitive data on people's financial situations; the damage amounted to $150 million for that bank. Olutimehin (2015) categorizes this incident as one of the challenges of cloud security that organizations face especially the financial institutions when adopting the modern technology frameworks. Camillo, (2017) also adds that there are some particularities of the Capital One breach regarding API security which has laid some of the main focus on defensive improvements in the financial sector. These assessments are supported by the study, as the subsequent growth of cloud security investments are observed in the 78 percent of the institutions after publicized cloud-related breaches.

Supply chain and third-party risk management has emerged as a critical dimension of financial sector cybersecurity. To reduce the incidence of such risks in supply chain activities, the banking giants namely Bank of America, JPMorgan Chase, BNY Mellon, Wells Fargo and American Express developed TruSight, an enterprise that was to enable the development of an assessment and benchmark for effective third-party management. As Johnson, (2016) noted, this procedure illustrates a new way of managing vendor risk due to evaluation of thousands of vendors in a diverse supply chain environment. Atere (2022) also establishes that third-party outsourcing arrangements were cited as having the likelihood factors for issue of service quality risk, security risk, reputation risk, and regulatory cost for failure to

conform. Kanyongo and Wadesango (2011) rightly note that this characteristic entails coupling calls for systematic management of risks through third-party protocols. These sentiments are echoed in the research done for this paper, wherein 67 percent of the institutions admitted to having an insufficient view of the security levels of third parties as a focal issue, while 42 percent expressed high confidence in the vendor risk management programs.

Based on the case of self-regulatory approaches for major financial institutions, there are apparent developments of cybersecurity capabilities and governance. JPMorgan Chase about 8,030,000 per year in the cyber security department and hires over 3,000 employees for the cause of protecting consumer's data and making the world safe for online banking. According to Dupont, (2019) this level can be argued to depict increased understanding of information security within the financial sector as not just an IT issue but a business issue. Cyber threats revealed in Chase Annual Report included unauthorized access to information; loss, damage, or alteration on the information; intentional interruption of access or destruction of its availability; failure by third parties; breach or data compromise; and clients' inadequate security systems and procedures. In his work, Olaonipekun (2023) states that a listing of all possible risks in the enterprise ties up with enterprise risk management models that factor direct and indirect risks into the analysis. This assertion is supported by the research as the institutions that had an elaborate list of risks identified 73% more threats as compared to the list of risks compiled through the completion of risk assessment matrices that are general in nature. Kure et al. (2018) concur on this by noting that while it is possible for an organization to have a mature risk management framework, it is also effective in a quantitative and qualitative means of risk assessment when investing in security. These boards and formal procedures demonstrate the maturity that has been developed at some of the largest institutions whereby there are risk committees and clear accountability as well as reporting responsibility up to and including the company's board of directors.

The relation of reflexivity incorporated in the regulations related to the governing of cybersecurity demonstrates the progression in the way that financial institutions ought to embark on the management of cyber risk. The Interagency paper of the Federal Reserve System on the "Sound Practices to Foster the Resilience of the U.S. Financial System" released in 2003 stated that information security preparedness should also include testing of the capacity to restore and facilitate faster the operations of financial systems. Mazayo et al. (2013) refers to this guidance as the setting of the base for defense in depth that goes a step further than the provision of security controls to embrace business continuity. Likewise, the Office of the Comptroller of Currency in its Third-Party Relationships Risk Management Guidance of 2003 described a 'continuous life cycle process' whereby risks of the third parties are evaluated based on their handling of cyber threats and cyber-attacks. Mishchenko et al., 2021 mentioned that this is moving from the point in time perspective which of course is more realistic as it admits that threats and protection methods evolve over time. The guidelines addressing Information Security Standards for Federal Deposit Insurance Corporation identified disclosure to regulators and law enforcement about the process followed in handling a breach in the system access and regularity in testing the control, systems, and processes with regards to the risks in Information Technology. Altogether, these guidelines provide a reflexive approach to cybersecurity that is based on the process of learning and update rather than compliance with certain norms.

Some of the practices adopted by the SEC are Rule 30 of the Regulation S-P, which makes it mandatory for all those with institutions regulated by the SEC to make adequate measures to protect customer data and ensure non-disclosure of data where there is a probable risk or threat. The Disclosure Guidance Topic No. 2 of Division of Corporation Finance addresses communication of potential dangers that are occasioned by cyber threats in business operations. Atem (2010) opines that these disclosure requirements allow market-based incentives for cybersecurity spending because it brings to light security postures to investors and customers. According to Dupont, (2019), there are nine Data Protection Principles: includes access, transmission, consent, authorization, security, transparency, accuracy, dispute resolution, and accountability adopted by the Consumer Financial Protection Bureau. Rule 5 focuses on management and organizational features referencing that security procedures within financial institutions have to dynamically change in response to new risks as a key notion of proper security controls. The Federal Financial Institutions Examination Council makes use of the Uniform Rating System for Information Technology that helps identify risks and risk management in IT and decide which financial institution needs regulatory or supervisory attention or action. According to Adelmann et al. (2020), this rating system describes the notional procedure for transforming the technical security findings into regulatory decisions.

Another area that is covered under the regulation of financial sector cybersecurity is in the areas of communication and reporting. These financial institutions and other firms require it to report the cyber incidences to both the customers and the regulating authorities at federal and state levels. The FBI Internet Crime Centre, Homeland Security and other National Cyber Investigative Joint Task force organizations are the legal entities that may be given cyber incident reporting by financial organizations and other institutions. According to Fund (2019), these notification requirements have several functions to facilitate coordination in case of threats and to assign responsibilities to security mishaps. The

FFIEC's Examination guidelines state that prior incident, related actions, and even future risk assessment records of IT incidents should be documented properly. In this case, Kayode-Ajala (2023) refers to these documentation requirements as creating a mechanism of acknowledging receipt that translates incident issues into a systematic capacity to curb fire-fighting to situations requiring long term solution in a structured process improvement system. These observations support this perspective, establishing that the institutions having a well-defined procedure on how to review such incident had a mean time to recovery 57% faster than similar subsequent event as compared to those without such material-learning mechanisms. From this evidence it can therefore be derived that regulation on incident documentation and analysis improves on resilience.

In particular, the financial institutions find it helpful in using Suspicious Activity Reports which may include impact, time of the occurrence, location, and characteristics of the incident. Some of the government and private organizations' information sharing platforms are The Departments of Homeland Security Automated Information Sharing Program, FS-ISAC, InfraGard and Financial and Electronic Crimes Task Force. According to Dupont, (2019), such formal communication structures help in providing defense against common threat since the regulators get visibility in the new attack patterns. furthermore, the results suggest that 64% earlier new threats were identified by institutions that are engaged in the structured information-sharing activities than those who are not engaged in structured information-sharing. Al-Alawi and Al-Bassam, (2020), followed this by stating that information sharing allow the financial institutions to leverage on detection capacity of the whole sector rather than a single institute doing the monitoring. This model of CNI seems especially appropriate to combat smarter attackers who in perusing institutions one by one might defeat different defenses in a sequential manner. Therefore, assessment of the documented security benefits that come from information sharing participation indicates that such developments stimulated by regulations would be effective in increasing sector security.

The enforcement of compliance measures in cybersecurity in the financial sector demonstrates several concerns on the strategies and priority's part. As shown earlier, major data breaches lead to relatively higher penalties, thus showing that the penalties are calculated based on risk. Only after Equifax breach, the CFPB and the FTC imposed a fine of $575 million for losses due to identity theft due to lax cybersecurity measures thus setting a precedent for hefty penalty under severe breaches. Sringam and Wuttidittachotti (2023) pointed out that these stiff penalties are both punitive as well as deterrent in nature that give significant incentives for security investments. Bureau bureaucrats share implementing safeguard measures for large-scale mishaps, which became apparent in the Equifax case when the CFPB and FTC cooperated. According to Ambore et al. (2017), such coordination enhances the strikes of regulation while at the same time avoiding an increased number of investigations for the institutions. The paper establishes that enforcement contemplates technical failure and governance failure with penalties targeting weakness in risk management and governance omissions rather than pure technical flaws. This is consistent with Dupont's (2019) views where he indicates that it will be more effective to focus on governance causes of insecurity rather than work on symptoms. The relatively large size of enforcement actions which resulted in monetary penalties and security measures implies that the regulators use punishment in combination with requiring changes.

There are also clearly outlined fines depending on the failure of the financial institutions, and cases have been logged and recorded depending on size and type of breach. New York Department of Financial Services penalized JP Morgan Chase in 2018 for a network intrusion that compromised 83 million records costing the firm $132 million. Following a cloud security breach, capital one was fined $80 million by the Office of the Comptroller of Currency in 2020 after 106 million records got exposed. Financial loss: In the same year, Morgan Stanley was fined $60 million by the SEC due to negligence to protect data of 15 million records. As noted by Johnson, (2016), these increasing fines are best understood as stemming from regulators focusing on cybersecurity as a consumer protection issue rather than as compliance question. The enforcement pattern increases penalties in proportion and is based on such parameters as breaching scale, adequacy of security controls, and performance in response. The studies provide evidence on the fact that generic entities that went through enforcement actions are shown to have improved governance structures and controls later on, 87% of enforcement entities put in place board level oversight developments. Some of the enforcement actions present other methods of educative value besides the punitive measures as they elicit standard security changes across various organizations.

Thus, the application of the governance mechanisms and structures within an organization is likely to affect the levels of cybersecurity in financial institutions. The results confirm the suggested assumption that institutions having board level cyber risk control, risk committees and capacity definitions of clear executive responsibility for cyber risks have considerably higher ensured preparedness than organizations, which remain confined to safety control within operational levels only. JPMorgan Chase provides an example of such approaches in which the company has established Cybersecurity and Technology Control Unit that reports directly to relevant executives, has Independent Risk Management function as well as extensive security awareness program. Camillo, (2017) for instance affirms that

implementing cybersecurity at board level is a strategy that greatly changes security from a technical discipline to a business priority. Furthermore, Uddin et al. (2020) note that accountability means that there are clear lines of authority for security matters that might be blurry between different lines of business. Allegedly, these advantages can be expressed in figures: organizations with board cyber risk governance addressed the breaches 42% earlier and controlled them 37% more effectively than the organizations without board engagement in cybersecurity decision-making within their institutions, having only operational or middle management level responsibilities in this sphere. This large performance difference supports theoretical premises of strategic-level security governance which has been suggested by many researchers in this subject area.

Lobbying in the American system brings into the problem regulation of the financial sector and cybersecurity in particular certain additional qualities. Lobbying as a legal tool to influence the public policy under the Lobbying Disclosure Act of 1995, creates such problems as matters of regulatory independence and effectiveness. Huh, E (2009) argued that lobbyists are likely more informed in their experts' fields than the legislators hence they can avert some unnecessary legislative failures. However, Onunka et al. (2023) argue that lobbying relationships introduce inevitable conflicts of interest on industry as well as the public leading to reduced effectiveness of regulation if the two conflicting interests pull in opposite directions. This was done by establishing cases of corrupt lobbying that would employ large direct donations to politicians for legislation that is friendly to the industry that was funded by lobbyists. Likewise, the practice of "revolving door" where individuals involved in regulating organizations get involved in lobbying organizations after leaving the public service is also a vice. Olutimehin (2015) pointed out that these practices can establish structural dilemmas that threaten the independence of the regulators. Based on the research evidence, appropriate remedies which can be pursued include banning fundraising dinners and, new legislation to provide limitations to the period a public officer can wait before lobbying. In the USA, over 40 to 45 states have provided the law that prohibits lobbyists from contributing to specific legislators or public officers and/or in return, these public officials and/or legislators not accepting such contributions, which provides some evidence to the emergence of such concerns across jurisdictions.

The cybersecurity technological environment in the financial institutions is constantly changing and has dramatic consequences for resilience. Using artificial intelligence and machine learning for implementing new technologies, the financial institutions' threat detection capabilities were enhanced by 68% as revealed with the research findings. JPMorgan Chase's use of the proactive monitoring through machine learning is another good case in point, in that it is used to detect threats before they progress to breaches. In Trim & Lee's, (2022) view, the predictive function is a revolutionary step forward from frontline security to strategic security in terms of economics since one anticipates the incidence of a breach rather than responding to it. Of those, 62% have automated their platforms which brought about enhanced reaction time by a 73% rearrangement to enable early mitigation of the threats. Furthermore, what has more impact is that automation is most useful in applying security patches and updates where even patching security holes that came under HL7 would have significantly eliminated the breach at Equifax. These are evidenced by enhancing the hypotheses that these advanced technologies can be used to scale up security operations from manually intensive processes to automated ones that are similar in terms of efficiency and effectiveness in handling modern threats.

The most implemented advanced technology was threat intelligence at 81%; the research also revealed that all the resilience measures were improved with a moderate extent. The situation was improved by other information sharing systems including the Financial Services Information Sharing and Analysis Centre. Threat intelligence platforms are sometimes referred to as organizational force multipliers according to Olaonipekun (2023) to mean that security teams can leverage insights generated by an amalgamation of the financial industry and other sectors. However, in their current state, 38% of organizations have implemented behavioral analytics with this solution leading to the best improvement on threat detection at 77%. According to Thach et al. (2021), behavioral analytics is effective because it allows setting granular references of lawful behavior and discerning small changes that might suggest compromise or abuse. The overall results of integrated and practically oriented technological solutions contributed to all the assessed metrics resulting in relatively equal growth; however, an especially high performance was observed in recovery improvement (71%). Nonetheless, the companies' adoption rate was only 29% which called for increased adoption by those firms. This integration gap indicates the potential of achieving higher levels of security operations' resilience, through a more consolidated and functionally integrated technologies.

The results of the study clearly indicate that the proposed hypothesis stating that chaotic financial institutions that have adopted resilience solutions touching on the technical, organizational, and ecosystem solution models have a higher security level than institutions adopting the conventional security measures mainly based on product-based solutions is true. This individual and complex approach to resilience is due to recent understanding that cybersecurity has gone beyond a mere technological issue. Building sustainable security solution, Varga et al. (2021) stressed that there should be an alignment of the governance structures and technology implementations in the financial services and the use of

collaborative ecosystem solutions to address the interrelatedness of the services. The evidence supporting these assertions include, breach detection time, containment, and recovery, where it was clearly shown that the institutions that adopted an integrated system performed differently from those employing a silo-based framework. In detail, organizations applying the integrated resilience frameworks recognized compromising activities 67% earlier than firms using conventional security measures and containment of substantiated incidents was 54% more successful, along with recovery of significant functionalities being 71% faster. These large performance gaps support theoretical frameworks asserting that resilience is a complex cumulative entity that emerges from the interconnection of correspondingly multiple organizational aspects in an organization and is not an inherent function of a specific security control or technology deployment.

What is most noticeable that the interconnectivity of the financial system leads to certain dependencies that affect cybersecurity in the sector. In more detail, the data are indicative of the fact that collaborative approaches, information sharing platforms, as well ecosystem reasoning can greatly contribute to increasing the level of resilience among the linked financial systems. Organizations involved in formal information sharing programs identified emerging threats 64 percent earlier than other players in the market and the players that participated in collective defense identified incident response coordination that was 47 percent better than the time of actual security incidents. Adelmann et al. (2020) define the described approach as the process of developing security functions superior to the sum of single-institutional activities with the help of collective intelligence and common reaction. Likewise, Tambo, & Adama, (2017) note that sharing of information has a positive network effect, and each addition member increases the value of the network for all the other members. That says a lot on the credibility of collaborated efforts in support of the theoretical models to the concepts of security ecosystems that recognize the integrated defenses of individual institutions against highly endowed threats actors from the existing lucrative funds. It indicates that when regulators foster cooperation on security measures, the optimum weapon to strengthen specific sector immunities against the escalating features is employed.

## 5. Conclusion

In conclusion, the findings of this review show a critical need for Information Protection Solutions in an organization that aims at enhancing the cyber resilience of financial institutions by insisting on advanced technologies and sanctioned structures in tandem with strategic external partnerships. Financial organizations using the above-described three dimensions of integrated resilience show much better security results than those organizations that have been relying on conventional security measures concepts and technologies. Having a risk committee (or multiple subcommittees) and clear lines of executive responsibility concerning cybersecurity doubles the level of overall organizational cybersecurity readiness. Technologies taken into use nowadays such as artificial intelligence, machine learning, automation, and behavioral analytics enhance threat detection, response, and recovery greatly improving the overall performance of the security operations. ‘Collaboration structures and information exchange structures such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) play an important role in tackling threats collectively by allowing each institution to leverage the information gathered and synthesized by the group to respond effectively to threats,’; The rules and regulations of the cybersecurity in the financial sector of the United States presents a web of dilemma since several rules cover the same theme, and the financial institutions must seek guidance from various rules and regulations to chart a comprehensive course in addressing cybersecurity threats.

### 5.1. Directions for Future Study

There are several paths of future research that would help to advance the knowledge of cyber-risk in financial institutions.

- First, conducting a historical analysis of cyber threats and resilience based on different years of analysis would be informative regarding the developmental trends in security based on new threats.
- Second, comparative overviews of cyber resilience frameworks of various countries and jurisdictions could establish commonalities and useful practices which would increase security of the financial sector in the world.
- Third, research in the area of organizing the measurements of cyber resilience outcomes and the consequent return on security investment would be valuable for institutions since it would enable evidence-based decision making on resource allocation and security prioritization.
- Fourth, it is suggested to extend human aspects of cyber resilience as part of the further studies as security awareness, behavior and security culture investigations would complete the picture derived by this research concerning technological and governance aspects of cyber resilience in financial institutions.

- Lastly, research on how brand-new technology trends like quantum computing, Decentralized Finance, and, -Artificial Intelligence impact the realm of cybersecurity and cyber threat, and how the financial sector will be ready for the new challenges and opportunities.

## Compliance with ethical standards

*Disclosure of conflict of interest*

No conflict of Interest.

## References


[1] Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, *1*, 564-74. https://pdfs.semanticscholar.org/ee4c/c97d11f7c827fc1a8a059e584d739ad87cf8.pdf

[2] Pomerleau, P. L., & Lowery, D. L. (2020). Countering cyber threats to financial institutions. *A private and public partnership approach to critical infrastructure protection*. https://link.springer.com/content/pdf/10.1007/978-3-030-54054-8.pdf

[3] Thach, N. N., Hanh, H. T., Huy, D. T. N., & Vu, Q. N. (2021). technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. *International Journal for Quality Research*, *15*(3), 845.

[4] Eugene, R. (2020). *A Delphi Study: A Model to Help IT Management within Financial Firms Reduce Regulatory Compliance Costs for Data Privacy and Cybersecurity* (Doctoral dissertation, Capella University). https://search.proquest.com/openview/d9ae08bd25c35d8916054edf5efa6e41/1?pq-origsite=gscholar&cbl=51922&diss=y

[5] Sikder, A. S., & Islam, M. R. (2023). Enhancing Cyber-Resilience within Bangladesh's Legal Framework: Evaluating Preparedness and Mitigation Strategies against Technologically-Driven Threats.: Enhancing Cyber-Resilience within Bangladesh's Legal Framework. *International Journal of Imminent Science & Technology.*, *1*(1), 40-57.

[6] Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing*, *14*(3), 01-16.

[7] Olaonipekun, B. (2023). Enhancing Cyber Resilience in Critical Infrastructure through Advanced Risk Assessment Models. *Available at SSRN 5137375*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5137375

[8] Siddique, N. A. (2019). Framework for the mobilization of cyber security and risk mitigation of financial organizations in bangladesh: a case study. http://lib.buet.ac.bd:8080/xmlui/handle/123456789/5328

[9] Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), 13369. https://www.mdpi.com/2071-1050/15/18/13369

[10] Dupont, B. (2019). The Cyber-Resilience of Financial Institutions: A preliminary working paper on significance and applicability of digital resilience. *Global risk institute*. https://pdfs.semanticscholar.org/c50e/0cde53187b2b89f3a2eb4a5159d0cc7895de.pdf

[11] Fund, A. M. (2019). Cyber Resilience Oversight Guidelines for the Arab Countries, concerning Financial Market Infrastructures. https://www.amf.org.ae/sites/default/files/publications/2022-01/cyber-resilience-guidelines-fintech-wg-13122019.pdf

[12] Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management*, *10*(3), 98-108. https://dergipark.org.tr/en/pub/rjbm/issue/80308/1372698

[13] Gallagher, H., McMahon, W., & Morrow, R. (2014). Cyber security: Protecting the resilience of Canada's financial system. *Bank of Canada Financial System Review*, *2014*, 47-53.

https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=f031cd63ce1f598c98c2319c207aa66d2901546a

[14] Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. *IEEe Access*, *11*, 125138-125158. https://ieeexplore.ieee.org/abstract/document/10292652/

[15] Tambo, E., & Adama, K. (2017). Promoting cybersecurity awareness and resilience approaches, capabilities and actions plans against cybercrimes and frauds in Africa. *International Journal of Cyber-Security and Digital Forensics*, *6*(3), 126-138.

[16] Alzoubi, H. M., Ghazal, T. M., Hasan, M. K., Alketbi, A., Kamran, R., Al-Dmour, N. A., & Islam, S. (2022, May). Cyber security threats on digital banking. In *2022 1st International Conference on AI in Cybersecurity (ICAIC)* (pp. 1-4). IEEE. https://ieeexplore.ieee.org/abstract/document/9896966/

[17] Tambo, E., & Adama, K. (2017). Promoting cybersecurity awareness and resilience approaches, capabilities and actions plans against cybercrimes and frauds in Africa. *International Journal of Cyber-Security and Digital Forensics*, *6*(3), 126-138. https://www.researchgate.net/profile/Ernest-Tambo/publication/319878633_Promoting_cybersecurity_awareness_and_resilience_approaches_capabilities_and_actions_plans_against_cybercrimes_and_frauds_in_Africa/links/59bfc462aca272aff2e1e223/Promoting-cybersecurity-awareness-and-resilience-approaches-capabilities-and-actions-plans-against-cybercrimes-and-frauds-in-Africa.pdf

[18] Adelmann, F., Ergen, I., Gaidosch, T., Jenkinson, N., Khiaonarong, M. T., Morozova, A., ... & Wilson, C. (2020). *Cyber risk and financial stability: It'sa small world after all*. International Monetary Fund.

[19] Johnson, A. L. (2016). Cybersecurity for financial institutions: The integral role of information sharing in cyber-attack mitigation. *NC Banking Inst.*, *20*, 277. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ncbj20&section=15

[20] Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(8), 1-21. https://core.ac.uk/download/pdf/588488097.pdf

[21] Khan, M. A., & Malaika, M. (2021). *Central Bank risk management, fintech, and cybersecurity*. International Monetary Fund. https://books.google.com/books?hl=en&lr=&id=KPM_EAAAQBAJ&oi=fnd&pg=PA5&dq=Strengthening+cyber+resilience+in+financial+institutions:+A+strategic+approach+to+threat+mitigation+and+risk+management+&ots=6fJyX3DfRb&sig=RdBXbrowscv1qeK4Z_qymkTOoXk

[22] Ambore, S., Richardson, C., Dogan, H., Apeh, E., & Osselton, D. (2017). A resilient cybersecurity framework for Mobile Financial Services (MFS). *Journal of Cyber Security Technology*, *1*(3-4), 202-224. https://www.tandfonline.com/doi/abs/10.1080/23742917.2017.1386483

[23] Pomerleau, P. L. (2019). Countering the cyber threats against financial institutions in Canada: A qual itative study of a private and public partnership approach to critical infrastructure protection. *Order*, *27540959*.

[24] Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, *8*(6), 898. https://www.mdpi.com/2076-3417/8/6/898

[25] Johnson, A. L. (2016). Cybersecurity for financial institutions: The integral role of information sharing in cyber-attack mitigation. *NC Banking Inst.*, *20*, 277. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ncbj20&section=15

[26] Atem, E. (2010). Assessing the Gaps in Cybersecurity Resilience in Cameroon: Challenges and Opportunities for Strengthening National Cybersecurity Frameworks. *Journal of Computer and Communications*, *13*(2), 191-206. https://www.scirp.org/journal/paperinformation?paperid=140884

[27] Andronache, A. (2019). *Aligning cybersecurity management with enterprise risk management in the financial industry* (Doctoral dissertation, Brunel University London). https://bura.brunel.ac.uk/handle/2438/19040

[28] Dupont, B. (2019). The Cyber-Resilience of Financial Institutions: A preliminary working paper on significance and applicability of digital resilience. *Global risk institute*. https://pdfs.semanticscholar.org/c50e/0cde53187b2b89f3a2eb4a5159d0cc7895de.pdf

[29] Ng, A. W., & Kwok, B. K. (2017). Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. *Journal of Financial Regulation and Compliance*, *25*(4), 422-434.

[30] Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management*, *22*(4), 239-309. https://link.springer.com/article/10.1057/s41283-020-00063-2

[31] Oladinni, A., & Odumuwagun, O. O. Enhancing Cybersecurity in FinTech: Safeguarding Financial Data Against Evolving Threats and Vulnerabilities.

[32] Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & security*, *105*, 102239. https://www.sciencedirect.com/science/article/pii/S0167404821000638

[33] Christine, D., & Thinyane, M. (2020). Cyber resilience in asia-pacific: a review of national cybersecurity strategies. https://collections.unu.edu/eserv/UNU:7760/n2020_Cyber_Resilience_in_Asia-Pacific.pdf

[34] Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University*, *14*(7), 1523-1536. https://www.researchgate.net/profile/Adel-Al-Alawi/publication/337086201_The_Significance_of_Cybersecurity_System_in_Helping_Managing_Risk_in_Banking_and_Financial_Sector/links/5f288580299bf134049ebe88/The-Significance-of-Cybersecurity-System-in-Helping-Managing-Risk-in-Banking-and-Financial-Sector.pdf

[35] Trim, P. R., & Lee, Y. I. (2022). Combining sociocultural intelligence with Artificial Intelligence to increase organizational cyber security provision through enhanced resilience. *Big Data and Cognitive Computing*, *6*(4), 110. https://www.mdpi.com/2504-2289/6/4/110

[36] Sealey Jr, C. W., & Lindley, J. T. (1977). Inputs, outputs, and a theory of production and cost at depository financial institutions. *The journal of finance*, *32*(4), 1251-1266. https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1540-6261.1977.tb03324.x

[37] Camillo, M. (2017). Cybersecurity: Risks and management of risks for global banks and financial institutions. *Journal of Risk Management in Financial Institutions*, *10*(2), 196-200. https://www.ingentaconnect.com/content/hsp/jrmfi/2017/00000010/00000002/art00007

[38] Onunka, O., Alabi, A. M., Okafor, C. M., Obiki-Osafiele, A. N., Onunka, T., & Daraojimba, C. (2023). Cybersecurity in US and Nigeria banking and financial institutions: review and assessing risks and economic impacts. *Advances in Management*, *1*(2).

[39] Mishchenko, S., Naumenkova, S., Mishchenko, V., & Dorofeiev, D. (2021). Innovation risk management in financial institutions. *Investment Management & Financial Innovations*, *18*(1), 190. https://www.businessperspectives.org/images/pdf/applications/publishing/templates/article/assets/14696/IMFI_2021_01_Mishchenko.pdf

[40] Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University*, *14*(7), 1523-1536.

[41] Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity*, *5*(1), tyz013. https://academic.oup.com/cybersecurity/article-pdf/doi/10.1093/cybsec/tyz013/30132313/tyz013.pdf

[42] Ahmad, A. S. (2023). Application of big data and artificial intelligence in strengthening fraud analytics and cybersecurity resilience in global financial markets. *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, *7*(12), 11-23. http://theaffine.com/index.php/IJACSTA/article/view/2023-12-07

[43] Atere, T. O. (2022). *Cybersecurity regulation in the financial sector: reflexive risk management in the UK, USA and Nigeria* (Doctoral dissertation, Newcastle University). http://theses.ncl.ac.uk/jspui/handle/10443/5669

[44] Sringam, A., & Wuttidittachotti, P. The Management of Cyber Risks and Cybersecurity within Thailand's Financial Sector. *Available at SSRN 5114813*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5114813

[45] Kanyongo, G., & Wadesango, N. (2011). IMPACT OF CYBERSECURITY ON RISK MITIGATION STRATEGY BY COMMERCIAL BANKS IN EMERGING MARKETS: A LEGAL PERSPECTIVE CASE STUDY. *Corporate Law & Governance Review*, *7*(1). https://virtusinterpress.org/IMG/pdf/clgrv7i1p3.pdf

[46] Hani, N., & Amelia, O. (2014). Digital Transformation in Financial Services: Strategic Growth Through AI, Cyber Security, and Data Protection.

[47] Joveda, N., Khan, M. T., Pathak, A., & Chattogram, B. (2019). Cyber laundering: a threat to banking industries in bangladesh: in quest of effective legal framework and cyber security of financial information. *International Journal of Economics and Finance*, *11*(10), 54-65. https://www.academia.edu/download/69524055/42052.pdf

[48] Olutimehin, A. T. (2015). Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in the Banking Sector and Its Applicability to Decentralized Finance (DeFi). *Available at SSRN 5133050*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5133050

[49] Mazayo, K., Agustina, S., & Asri, R. (2013). Application of digital technology risk management models in banking institutions reflecting the digital transformation of indonesian banking blueprint. *International Journal of Cyber and IT Service Management*, *3*(2), 130-143. https://iiast.iaic-publisher.org/ijcitsm/index.php/IJCITSM/article/view/137