INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 9, Issue 6 - V9I6-1197)
Available online at: https://www.ijariit.com

From Risk to Resilience: Strengthening Cyber Security in Financial Institutions

Silvia Tsovwen Asakpa
silviaasakpa@gmail.com
Richard Chaifetz School of Business, Saint Louis University, St. Louis, United States

ABSTRACT

The study examines the escalating cyber threats facing financial institutions, particularly the surge in state-sponsored attacks and vulnerabilities exacerbated by the pandemic's shift to remote services. Notably, ransomware incidents have surged, and transnational crime groups now exploit specialized tools. Despite robust regulatory frameworks like GLBA, FFIEC, PCI-DSS, and NIST Cybersecurity, financial entities grapple with defending against evolving threats. The study emphasizes the imperative of prioritizing cyber resilience strategies and strict adherence to regulations. Advanced measures such as encryption, machine learning, and real-time monitoring are proposed to fortify security measures. It advocates for continuous staff training to enhance awareness and adherence to evolving cybersecurity practices. Moreover, the article underscores the significance of regular risk assessments for identifying vulnerabilities and ensuring timely updates to security measures against evolving threats. Collaboration among institutions is advocated to strengthen collective defenses, enabling a unified response to cyber incidents and bolstering the overall cybersecurity posture of the financial industry. In essence, the article highlights the necessity for financial institutions to proactively embrace comprehensive strategies that encompass resilience, regulatory compliance, technological advancements, and collaborative efforts to effectively combat escalating cyber threats.

Keywords *— Cybersecurity, Financial Institutions, Cyber Threats, Cyber Resilience, Ransomware, State-sponsored Attacks, Financial Sector, Regulatory Framework, Encryption, Cyber Risk.*

I. INTRODUCTION

In recent years, cyber threats confronting financial institutions have proliferated. Among the overall volume of cyber-attacks, there has been a noticeable rise in state-sponsored cyber-attacks directed at the financial system. These attacks have escalated in frequency, sophistication, and impact, displaying an unexpected and accelerated surge. The primary catalysts for this surge in cyber-attacks were the pandemic and an amplified dependence on remote services (Olivér & Gábor , 2023).

The financial services sector stands as a primary target for hackers. As indicated by the Modern Bank Heist 3.0 survey, 80 percent of the surveyed financial institutions noted a surge in cyber-attacks, marking a 13 percent increase compared to 2019. Additionally, 82 percent of these institutions highlighted the heightened sophistication of cybercriminals, with malware being employed in longer and more intricate campaigns (Tom and Ryan, 2020).

Another survey underscored the disproportionate impact of ransomware attacks on the banking industry. In the first half of 2021 alone, there was a staggering year-on-year increase of 1,318 percent in these attacks (Henriquez, 2021). According to insights from the Modern Bank Heist survey, the ultimate objective is to utilize native operating system tools to remain undetected or to establish a presence in one system, enabling the attackers to 'island hop' onto a larger, more lucrative target. Attackers breach one network and leverage it to gain access to an affiliated network, occasionally exploiting supply-chain partners' systems for this purpose (Tom and Ryan, 2020).

According to OFR (2017), cybersecurity incidents can disrupt the operations of a financial firm that provides critical services, reduce confidence in firms and markets, and damage the integrity of key data.

Transnational organized crime groups are increasingly utilizing specialized cybercrime tools and services to perpetrate a wide array of offenses against financial institutions at an alarming pace. These crimes include ransomware campaigns, distributed denial of service (DDoS) attacks, and business email compromise (BEC) scams. Criminals are collaborating more frequently, sharing resources and information, and funneling their illegal profits into the development of even more potent capabilities. The proliferation of off-the-shelf malware has opened doors for inexperienced criminals to initiate their own illicit operations. This trend, coupled with the continual commercial expansion of mobile devices, cloud-based data storage, digital payment systems, and services, provides cybercriminals with an ever-expanding array of avenues to exploit for attacks.

Every organization, especially those in financial services, must maintain a high level of vigilance against these evolving threats. Establishing and sustaining an ongoing dialogue with law enforcement is crucial to ensure swift action in the event of an incident (Tom and Ryan 2020).

The finance industry has been a pioneer in cybersecurity and fostering extensive information sharing and collaboration across the sector. Despite these proactive measures, there has been a surge in both the frequency and complexity of cyber-attacks targeting financial institutions and market infrastructures. Consequently, there has been a notable increase in security investments and a heightened emphasis on strategies to reduce and handle cyber risks. Simultaneously, stakeholders in the financial sector, including regulators and governments, have been striving to enhance overall resilience and stability. Their collective aim is to prevent a recurrence of crises akin to the financial meltdown experienced a decade ago.

Recently, cyber-resilience has garnered significant attention within cybersecurity discussions, despite its ambiguous nature, making it challenging to precisely define and assess. Its surge in popularity is undoubtedly associated with frequent headlines highlighting cyberattacks and data breaches across newspapers and technology platforms. These incidents underscore the vulnerability of our digital systems and the inability of organizations to safeguard the sensitive information entrusted to them. Even highly adept and security-focused entities are susceptible to severe cybersecurity breakdowns (Benoıt, 2019).

The idea of cyber-resilience presents an appealing alternative to the prevailing 'predict and protect' strategy that has dominated information security for decades. Faced with the harsh reality that no digital system can guarantee absolute invulnerability against continual attacks, organizations are acknowledging the necessity of creating procedures and technologies that help after significant breaches occur (Benoıt, 2019).

Problem

In today's technological landscape, the banking sector relies significantly on sophisticated digital systems to deliver prompt and efficient financial services to customers (Gosling, 2020). However, this heavy reliance exposes financial institutions to potential risks, especially concerning the security of customer data and the threat of financial fraud. Protecting customer information and preventing fraudulent activities have become pivotal concerns for financial institutions operating within the United States (Grupo, 2021). Jonah Force Hill, the senior cyber policy advisor and executive director of the U.S. Secret Service Cyber Investigations, stated that in 2023, virtually every sector across the global economy experienced some form of cybercrime. Among these sectors, none faced more consistent targeting than the financial sector (Olivér & Gábor , 2023).

Financial institutions store large volumes of sensitive customer data, encompassing personal information, account details, and financial transaction records. This makes them primary objectives for cybercriminals seeking unauthorized entry for fraudulent purposes like identity theft or financial exploitation (Luecking et al, 2020). Successful cyber-attacks can yield severe repercussions, leading to financial losses for both individuals and institutions, alongside damaging reputational harm and potential legal ramifications (PWC, 2021).

The escalating risk of cyber threats directed at the banking sector has been notable. Hackers and criminal entities have heightened their sophistication levels, utilized advanced tactics and exploited weaknesses within banking systems and their infrastructure. The continuously evolving threat landscape encompasses various dangers, including malware attacks, phishing schemes, ransomware incidents, and insider threats, among others (Frost & Sullivan, 2020). These risks not only jeopardize the confidentiality and integrity of customer data but also erode confidence in the banking industry.

II. LITERATURE REVIEW

Cyber Resilience

Embracing a compelling analogy, organizations, upon recognizing that they exist in a perpetual state of cyber-vulnerability despite deriving substantial productivity benefits from the technologies that also pose threats, must learn to "survive on a diet of poisoned fruit" (Danzig, 2014). This dilemma of effectively responding to and managing disruptions caused by unpredictable adverse events, which have the potential to destabilize and potentially eliminate, is not unique to the cyber domain or specific to financial institutions. It has been a central challenge for all intricate ecological, social, organizational, and technical systems.

The solution lies in resilience, temporarily defined as the capability to endure, recover from, and adjust to external shocks. Echoing the sentiments of a foundational figure in the concept (C.S. Holling, a Canadian ecologist), this shift in perspective "does not demand an exact ability to foresee the future, but rather a qualitative ability to devise systems capable of assimilating and accommodating future events in whatever unexpected guise they may appear" (Holling, 1973).

The need for cyber-resilience within the financial sector

Cyberattacks have evolved into an unavoidable digital threat, persisting regardless of the significant investments made by highly developed financial institutions in cutting-edge security technologies (Conference Board of Canada, 2018). Understanding the urgency of cyber-resilience requires examining recent disruptive incidents targeting these institutions. Of particular significance are the various motives driving these attacks, the varying levels of technical expertise demonstrated by the attackers, and the impact—both individual and collective—on the organizations affected. These considerations shed light on why, within such a complex and unpredictable risk landscape, the conventional security approach, centered on the unachievable goal of preventing or halting cyberattacks, is ineffective. Instead, a more pragmatic and realistic paradigm must be embraced, one in which organizations learn to coexist with these disruptive threats (Tedim and Leone, 2017)

Cyber Risk

Cyber risk can be defined based on three parameters: firstly, "Impact" quantifies the potential damage a risk might cause; secondly, "Threat" determines the likelihood of a particular risk occurring; thirdly, "Vulnerability" gauges the effectiveness of current information security measures (Biener, , Eling, & Wirfs, 2015). The significance of cyber risk is consistently growing, as indicated by the rising number of scholarly articles dedicated to this subject across various disciplines including computer science, engineering, business management, economics, and social sciences (Strupczewski, 2021). The concept of cyber risk encompasses two dimensions: technical and economic. From a technical perspective, it involves intricate design complexities, the (re)programmable nature of networked components, and a dynamically evolving global threat landscape. In an economic context, key elements of cyber risk include incomplete information, externalities, and correlations arising from shared risk factors (Böhme, Laube, & Riek, 2018).

Cybersecurity Risks in the US Financial Sector

Financial institutions in United States face a wide range of cyber threats that significantly threaten their operations and the privacy of customer data. Understanding these threats is crucial for developing strong cybersecurity strategies. Some of these threats include:

1. **Malware Attacks:** Malicious software, known as malware, remains a persistent threat to banking systems, often aiming to infiltrate and compromise these systems, leading to unauthorized access and the theft of sensitive information (FS-ISAC, 2022). This category encompasses a range of harmful software, including viruses, worms, and Trojans, posing an enduring risk to the security of the financial industry.

2. **Phishing and Social Engineering:** Phishing attacks represent a prevalent and concerning cyber threat that targets bank customers and employees through fraudulent emails or messages designed to deceive recipients. The primary objective is to trick individuals into divulging confidential information or engaging in unauthorized transactions. Social engineering tactics, like impersonation and manipulation, are frequently employed to manipulate individuals and obtain sensitive data (Verizon, 2021).

3. **Distributed Denial of Service Attacks (DDoS):** These attacks aim to disrupt client access to financial services by overwhelming networks with an enormous volume of traffic. Mitigating the impact of such attacks proves challenging due to the utilization of botnets, which are networks of compromised devices controlled by cybercriminals. Botnets are commonly employed to orchestrate these attacks, adding complexity to efforts aimed at reducing their impact (Efijemue , et al., 2023).

4. **Insider Threats:** The banking sector faces threats from individuals within their own ranks employees or contractors who possess access to sensitive data and might intentionally or unintentionally compromise the security of customer information. Insider threats encompass various activities, including data theft, unauthorized access, or the accidental disclosure of confidential information. These risks arise from individuals within the organization who may purposefully or inadvertently undermine the security of sensitive data (CERT, 2023).

Risks posed by Cybersecurity to Financial Institutions

Lack of substitutability

The financial services sector heavily relies on a robust IT infrastructure to conduct transactions and facilitate payment transfers. Within these financial networks, a handful of firms or utilities act as central hubs. The services they provide would pose significant challenges if they were lost or disrupted. These pivotal hubs encompass central banks, custodian banks, and systems responsible for payment processing, clearing, settlement, and communication. Issues arising at these crucial hubs can potentially elevate concerns about financial stability. Historically, such instances have typically revolved around operational risks other than cyber threats. For instance, in 1985, the Bank of New York required a $23 billion discount window loan from the Federal Reserve to prevent market disruptions caused by a software failure, rendering the bank unable to return securities it had received from other institutions in an intermediary capacity (Ennis and Price, 2015). This incident marked the largest discount window loan at that time. A cyber event involving a financial entity providing critical services to other market participants could similarly generate systemic risks. Implementing policies that promote redundancy within the financial system can help mitigate these risks. Regulators should carefully consider such policies.

Loss of Confidence

Cyber attackers frequently aim at acquiring customer account details and financial assets. While most of these breaches have been isolated occurrences, impacting solely the targeted firm and its clientele, a more extensive breach could result in a broader loss of trust. For instance, in South Korea back in 2014, hackers managed to pilfer customer names, credit card details, and phone numbers from a credit rating agency. This news prompted numerous customers to contact or visit their banks, seeking assurance about the security of their information. Many individuals opted to cancel their credit cards as a precautionary measure. Despite this incident causing significant concern, it did not escalate into a full-fledged banking crisis (Sang-Hun, 2014).

Loss of data integrity

Maintaining the integrity of financial data holds paramount importance. Numerous financial markets operate on a just-in-time principle. Therefore, financial institutions require resilient backup data that can be swiftly restored following a cybersecurity event. Nevertheless, there are trade-offs involved in the swift recovery of data and ensuring that the restored information remains secure, precise, and does not exacerbate cyber risks, particularly in high-speed order processing markets. The corruption of data could potentially disrupt market operations and might pose challenges in terms of reversal or recovery (IOSCO, 2016).

Regulatory Framework for Cybersecurity in the US Banking Sector

1. **Gramm-Leach-Bliley Act (GLBA):** Enacted in 1999, the GLBA is a significant legislation within the financial sector. It imposes obligations on financial institutions to prioritize the protection of customer information. This act requires these institutions to establish and maintain robust information security programs. These programs are designed to secure sensitive data against unauthorized access, ensuring the confidentiality and integrity of customer information. By mandating these measures, the GLBA aims to enhance consumer trust by fostering a secure environment for financial transactions and interactions (FTC, 2022). The Gramm-Leach-Bliley Act (GLBA) includes a distinct Privacy of Consumer Financial Information Rule, directly impacting cybersecurity in financial services. This rule pertains to the collection of non-public personal information (NPI) by companies when offering or disclosing information about financial products or services. Non-compliance may result in fines of up to $100,000 per violation and potential imprisonment of complicit directors for up to five years (HYPR, 2023).

2. **Federal Financial Institutions Examination Council (FFIEC) Guidelines:** The FFIEC provides guidance that assists financial institutions in managing and mitigating cyber-security risks effectively. The Cybersecurity Assessment Tool offered by the FFIEC is a valuable resource enabling these institutions to assess their cyber-security posture comprehensively. Through this tool, institutions can identify potential vulnerabilities and areas requiring improvement, allowing them to prioritize and bolster their cyber defenses (FFIEC, 2023). The FFIEC, overseeing federally supervised financial institutions, establishes standards encompassing effective authentication and access risk management practices. Its cybersecurity best practices highlight the significance of multi-factor authentication (MFA) as a crucial security measure against financial losses and data breaches, aligning with the PSD2 Strong Customer Authentication directive. These standards refer to NIST guidelines SP 1800-17 and SP 800-63B, offering instructions for password less MFA based on FIDO specifications (HYPR, 2023).

3. **Federal Reserve System Guidance:** The Federal Reserve System's guidance emphasizes the importance of robust governance, efficient risk management practices, and collaboration with regulatory authorities to combat cyber threats. It underscores the necessity for financial institutions to establish strong internal controls, effective risk assessment processes, and cooperative engagement with regulatory bodies. This guidance aims to reinforce a proactive approach to cybersecurity, ensuring that financial entities are well-prepared to address evolving threats (Efijemue , et al., 2023).

4. **Payment Card Industry & Data Security Standard (PCI-DSS):** Although not exclusive to the banking sector, PCI-DSS is paramount for financial institutions engaged in credit card transactions. It lays down stringent security standards and protocols to safeguard cardholder data. Compliance with these standards is crucial to prevent unauthorized access, ensuring the secure handling and processing of credit card information. Adherence to PCI-DSS helps maintain trust between financial institutions and their customers by assuring the safe handling of sensitive financial data (PCI, 2020). The PCI DSS regulates payment processors

handling transactions for major credit and debit card firms. Financial services' cybersecurity programs must meet specific requirements, including safeguarding cardholder data, encrypting stored and transmitted data, and ensuring access authentication for system components. Violations of PCI DSS guidelines can lead to fines and limitations in accepting major credit cards (HYPR, 2023).

5. **National Institute of Standards and Technology Cybersecurity Framework (NIST CSF):** The NIST Cybersecurity Framework is a flexible and widely recognized guideline adopted by financial institutions. It serves as a comprehensive blueprint for these institutions to assess, manage, and enhance their cybersecurity posture. The framework's emphasis on risk management and continuous improvement empowers financial entities to adapt to evolving cyber threats, fostering a proactive and adaptive approach to cybersecurity (NIST, 2018).

6. **State Data Breach Notification Laws:** These laws, enacted by various states, require financial institutions to promptly inform customers in the event of a data breach compromising their personal information. The laws outline specific timeframes and criteria for notification, ensuring transparency and empowering affected individuals to take necessary precautions. These notifications contribute to rebuilding trust by demonstrating transparency and proactive efforts in handling data breaches (Efijemue , et al., 2023).

Approaches to Strengthen Cyber security in Financial Institutions

Encryption and Tokenization in Protecting Customer Data

Encryption and tokenization are robust tools crucial for safeguarding customer data in financial institutions. Encryption transforms data into an unreadable form that requires a decryption key for comprehension, while tokenization substitutes sensitive information with non-sensitive tokens, allowing secure processing (NIST, 2010; PCI, 2021).

Implementing encryption and tokenization techniques significantly strengthens the security of customer data during both storage and transmission. Prioritizing data privacy necessitates measures such as data classification, secure storage practices, safe transmission methods, and the adoption of encryption and tokenization strategies. These actions are vital for enhancing the protection of customer data, minimizing risks linked to data breaches and financial fraud (Efijemue et al, 2023).

By employing encryption and tokenization, financial institutions not only protect sensitive data but also ensure that unauthorized access does not enable interpretation or misuse of the information without the required decryption key or access to the original data. This layered security approach enhances overall customer information protection, aligning with regulatory standards and industry norms to uphold data privacy and integrity in financial services.

Adopting Fraud Detection and Prevention Techniques

Financial institutions employ various fraud detection and prevention techniques within cybersecurity to safeguard against potential threats.

Financial institutions utilize various methods for fraud detection and prevention:

1. **Machine Learning and AI-Based Systems:** These technologies analyze data, identifying fraud patterns and adapting to new trends for more accurate detection.

2. **Behavioral Analytics:** Monitoring user behavior detects abnormal activities indicating potential fraud.

3. **Biometric Authentication:** Unique user verification methods, like fingerprint or facial recognition, reduce unauthorized access risks.

4. **Transaction Monitoring:** Real-time tracking spots irregular spending or activities deviating from a user's typical behavior.

5. **Fraud Risk Scoring:** Assigning risk scores to activities prioritizes potential fraud cases for investigation.

6. **Device Recognition:** Identifying suspicious logins or activities from unrecognized or compromised devices enhances security.

7. **Customer Verification:** Multi-factor authentication (MFA) adds security layers, like SMS codes or tokens, to prevent unauthorized access.

8. **Collaboration:** Sharing insights and data on fraud trends among institutions strengthens defenses collectively.

9. **Continuous Training:** Regular updates and training programs ensure staff awareness of current fraud schemes and cybersecurity practices.

10. **Regulatory Compliance:** Adherence to industry regulations ensures the implementation of necessary security measures and protocols.

Anti-Money Laundering (AML) and Transaction Monitoring Strategies

Financial institutions employ robust AML (Anti-Money Laundering) strategies like KYC (Know Your Customer), due diligence, and enhanced transaction monitoring to meet regulations and uncover illicit activities. Effective fraud prevention involves collaboration with law enforcement, sharing fraud intel, and staying updated on emerging fraud techniques. Comprehensive fraud detection methods, including anomaly detection, machine learning, and behavioral analytics, bolster financial institutions' ability to prevent fraud and safeguard customer assets. Transaction monitoring is crucial for detecting and preventing financial fraud, wherein systems analyze transactions, identify suspicious patterns, and flag potential cases of money laundering or fraud (Efijemue , et al., 2023). Employee screening and background checks are crucial for identifying threats. Verifying history and records reveal potential risks, aiding in preventing insider threats and safeguarding sensitive data.

Using Block-chain Technology for Secure Transactions and Data Integrity

Blockchain's secure and transparent transactions, alongside its decentralized nature, serve cybersecurity applications. It is used for threat detection as AI and machine learning is used to analyze data for proactive cyberthreat identification. Block Chain technology enable behavioral analytics as it detects anomalies indicating malicious activities. AI automates incident response, reducing damage and response times, bolstering cybersecurity. Using blockchain technology improves data security, diminishes dependence on trusted third parties, and reinforces the cybersecurity infrastructure.

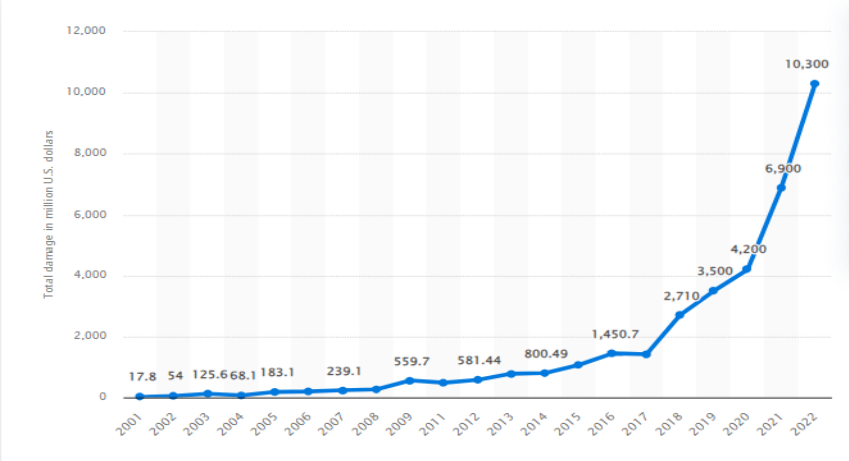
Real-time Monitoring and Threat Intelligence Sharing

Real-time monitoring and threat intelligence sharing are vital elements in cybersecurity. Continuous network and system monitoring, along with SIEM tools, detect potential threats promptly. Collaboration in sharing threat intel across sectors aids in identifying and mitigating cyber threats collectively. These practices enable proactive threat detection and incident response, reinforcing cybersecurity defenses. Embracing AI, ML, blockchain, and prioritizing real-time monitoring ensures organizations stay ahead in defending against evolving cyber threats and safeguarding critical assets (Efijemue , et al., 2023).

III. METHODOLOGY

This paper adopted descriptive tools of analysis to summarize the variables (cost incurred as a result of cyber-crimes, net income of banking industry and performance of finance industry (% of GDP). Correlation analysis is used to establish relationship and significance between cost of cyber-crimes and performance of finance industry. Data was collected through secondary sources such as Statista and Bureau of Economic Analysis. Times series data was adopted in the study and the data span between 2007 and 2022.

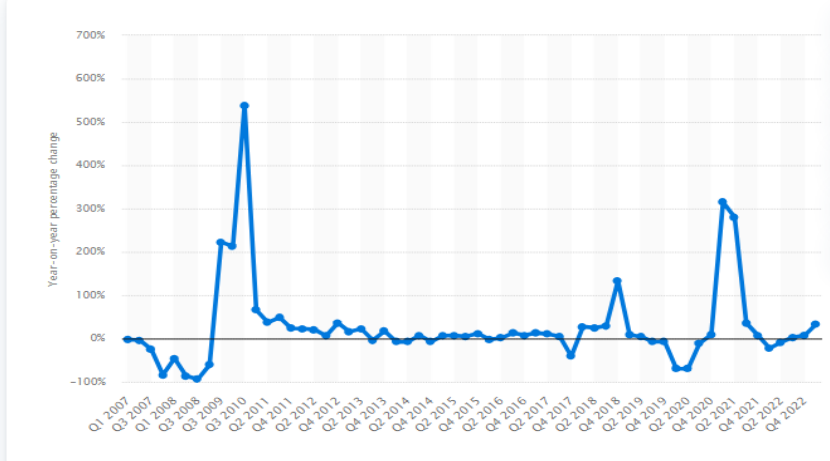
Monetary Damage Caused by Reported Cybercrime in the United States



Source: (Statista, 2023)

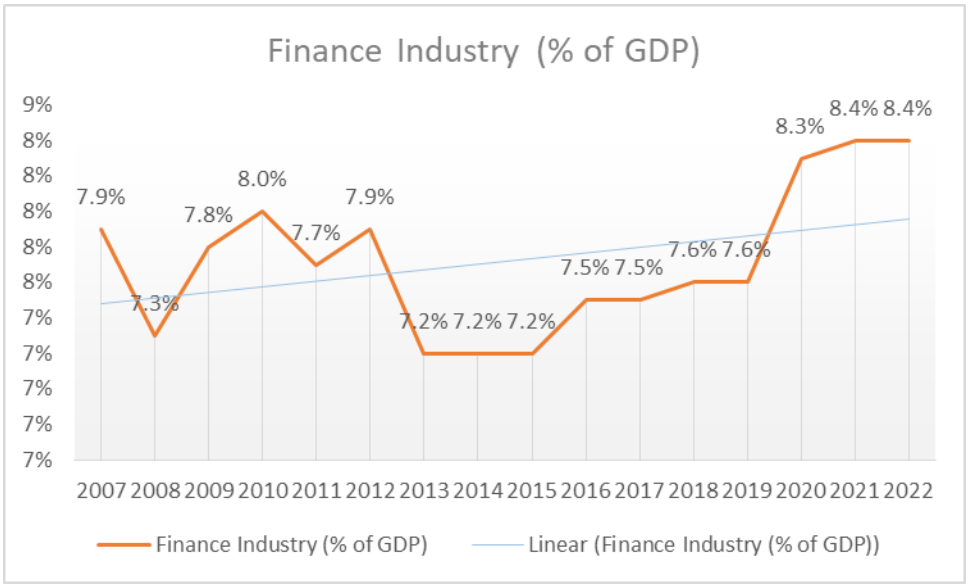
From 2001 to 2022, the monetary losses reported to the United States' Internet Crime Complaint Center (IC3) due to cybercrime exhibited a notable rise. In the latest documented period, complaints referred to the IC3 resulted in annual losses of $10.3 billion, an increase from $6.9 billion the previous year.

Percentage change on previous year of net income of the overall banking industry in the United States from 1st quarter 2007 to 1st quarter 2023



(Statista, 2023)

The U.S. banking industry, encompassing commercial banks and savings institutions, witnessed a sharper decline in net income in 2008 compared to 2022. During the third quarter of 2008, the industry's net income plummeted by 94 percent compared to the same quarter of the previous year, marking the lowest growth rate. Following the 2007/2008 global financial crisis, there was a significant resurgence in growth rates observed in 2009 and 2010. From 2011 to 2019, the growth rate remained relatively stable, showing fewer drastic fluctuations. However, the onset of the COVID-19 pandemic led to a decline in growth rates in 2020, followed by an increase in 2021. The first half of 2022 displayed a negative growth rate. As of the first quarter of 2023, the American banking industry witnessed a quarterly income growth rate of 33.6 percent.



Source: Author's Computation (2023)

The graph above shows the contribution of finance industry to GDP in US between 2007 and 2022. The linear line shows that over the years, there has been positive increase in contribution of finance industry to GDP. The contribution was between minimum of 7.2% and peak of 8.4% which was attained in 2021. Over the years, the sector's contribution between 2012 and 2015 (7.2%) was the least.

Table 1: Summary Statistics of Variables

	Cost of Cyber Crimes (US'M)	Finance Industry (%GDP)	Banking Sector (%)
Mean	2238.889	7.718750	0.421994
Median	935.6000	7.650000	0.062900
Maximum	10300.00	8.400000	3.758000
Minimum	239.1000	7.200000	-0.800500
Std. Dev.	2811.584	0.410234	1.080767
Skewness	1.830651	0.345964	2.013036
Kurtosis	5.448134	2.024599	6.788221
Jarque-Bera	12.93232	0.953449	20.37325
Probability	0.001555	0.620814	0.000038

The average annual cost of cybercrimes over the period was approximately $2.24 billion, with significant variability shown by a large standard deviation of approximately $2.81 billion. The data on cybercrime costs is positively skewed, indicating an asymmetrical distribution with a tail extending towards higher costs. This skewness is further evident from a high kurtosis value, suggesting a peaked and heavy-tailed distribution. Additionally, the Jarque-Bera test indicates a significant departure from a normal distribution, signifying non-normality in cybercrime cost data. The finance industry's average contribution to the Gross Domestic Product (GDP) stands at approximately 7.72%. This metric experiences relatively low variability, evident from a smaller standard deviation of about 0.41%. The skewness and kurtosis values suggest a slightly skewed and moderately peaked distribution, respectively. The Jarque-Bera test, with a high p-value of 0.62, indicates that this data closely adheres to a normal distribution. The banking sector's average percentage, concerning some aspect (possibly of GDP), stands at around 0.42%. However, there is a notable issue with the data as the minimum value is negative, potentially indicating a data anomaly. This sector demonstrates high variability, indicated by a considerable standard deviation of approximately 1.08%. The skewness and kurtosis values show a highly positively skewed and peaked distribution, suggesting a significant presence of outliers and non-normality in the data. The Jarque-Bera test confirms a substantial deviation from a normal distribution with a very low p-value of 0.000038.

The cost of cybercrimes varies significantly, with high variability, positive skewness, and kurtosis in the data. The finance industry's contribution to the GDP shows less variability and adheres more closely to a normal distribution. However, the percentage contribution of the banking sector demonstrates high variability, considerable skewness, and kurtosis, indicating potential data anomalies.

Correlation Analysis

Table 2: Correlations

		Cost of Cyber Crimes (US'M)	Finance Industry (% of GDP)
Cost of Cyber Crimes (US'M)	Pearson Correlation	1	.-673**
	Sig. (2-tailed)		.004
	N	16	16
Finance Industry (% of GDP)	Pearson Correlation	.-673**	1
	Sig. (2-tailed)	.004	
	N	16	16

**. Correlation is significant at the 0.01 level (2-tailed).

The correlation analysis above shows the relationship between monetary damaged caused by cybercrimes and performance of finance industry in US between 2007 and 2022. The correlation coefficient (0.673) revealed that there is negative relationship between annual costs incurred as a result of cyber crimes and finance industry. The relationship is significant as the probability value of the analysis (0.004) is less than 5% significance level.

The negative correlation implies that as the financial impact caused by cybercrimes increases, the performance of the finance industry tends to decrease. Moreover, the statistical significance of this relationship is confirmed by the probability value of 0.004, which is less than the conventional 5% significance level.

These findings suggest that higher annual costs incurred due to cybercrimes are associated with a notable decline in the performance of the finance industry. The negative correlation underscores the potential adverse effects that cybercrimes have on the industry's overall performance during the evaluated period. The negative correlation emphasizes the importance of robust cybersecurity measures within the

finance sector. Implementing effective cybersecurity protocols, investing in protective technologies, and enhancing cybersecurity resilience could potentially mitigate the financial impact of cybercrimes and, consequently, safeguard the industry's performance.

IV. CONCLUSION AND RECOMMENDATION

The financial sector has faced a significant surge in cyber threats, particularly state-sponsored attacks. The sophistication and frequency of these attacks have escalated, posing severe challenges to financial institutions. The pandemic-induced shift towards remote services has further exposed vulnerabilities, leading to an increased incidence of cyber-attacks targeting financial systems. Notably, ransomware attacks have seen a staggering increase, prompting attackers to exploit supply-chain partners' systems. The intent is to infiltrate systems and move from smaller targets to more lucrative ones. Transnational organized crime groups have developed specialized cybercrime tools, collaborating extensively to further enhance their capabilities and financial gains.

Cybersecurity incidents have far-reaching consequences, disrupting financial services, damaging market integrity, and eroding confidence in firms and markets. The heavy reliance on digital systems storing sensitive customer data makes financial institutions prime targets for cybercriminals. Successful attacks can lead to financial losses, reputational damage, and legal ramifications affecting individuals and institutions alike. Organizations are transitioning from a 'predict and protect' strategy to one that focuses on post-breach support. The concept of cyber-resilience has gained prominence as institutions recognize the limitations of solely preventive measures. Emphasizing post-breach support becomes crucial in mitigating the impact of cyber incidents. The banking sector faces multiple cyber threats, including malware attacks, phishing schemes, DDoS attacks, and insider threats, compromising data integrity and trust. Regulatory frameworks such as GLBA, FFIEC guidelines, Federal Reserve System guidance, PCI-DSS standards, NIST Cybersecurity Framework, and state data breach notification laws provide essential directives for effective information security, risk management, and collaboration against cyber threats.

It is therefore recommended that financial institutions must prioritize cyber resilience strategies to prepare for effective recovery post-breach, reducing the impact on operations and customer trust. Adhering strictly to regulatory frameworks like GLBA, FFIEC, PCI-DSS, and NIST Cybersecurity ensures robust information security and compliance, aiding defense against evolving threats. Implementing advanced measures such as encryption, machine learning, and real-time monitoring significantly fortifies security. Continuous staff training is vital to enhance awareness and adherence to cybersecurity practices. Regular risk assessments identify vulnerabilities, allowing timely updates to security measures against evolving threats. Collaboration among institutions strengthens collective defenses, enabling a unified response to cyber incidents and bolstering the overall cybersecurity posture of the financial industry.

V. REFERENCES

[1] Benoıt, D. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity, 5*(1), 1-17.

[2] Biener, , C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *Geneva Papers on Risk and Insurance, 40*, 131-158.

[3] Böhme, R., Laube, S., & Riek, M. (2018). A fundamental approach to cyber risk analysis. *Variance, 12*(2), 161-185.

[4] Efijemue , O. P., Obunadike , C., Olisah , S., Taiwo , E., Kizor-Akaraiwe , S., Odooh , C., & Ifunanya , E. (2023). Cybersecurity Strategies for Safeguarding Customer's Data and Preventing Financial Fraud in the United States Financial Sectors. *International Journal on Soft Computing (IJSC), 14*(4), 1-16.

[5] HYPR. (2023). *Top 12 Financial Services Cybersecurity Regulations to Know in 2023*. Retrieved 11 17, 2023, from https://blog.hypr.com/top-financial-services-cybersecurity-regulations

[6] Office of Financial Research. (2017). *Cybersecurity and Financial Stability: Risks and Resilience.*

[7] Olivér , G., & Gábor , K. (2023). Impact of cyber-attacks on the financial institutions. *Procedia Computer Science, 219*, 84-90.

[8] Statista. (2023). *Annual amount of monetary damage caused by reported cybercrime in the United States from 2001 to 2022*. Retrieved 11 18, 2023, from https://www.statista.com/statistics/267132/total-damage-caused-by-by-cybercrime-in-the-us/

[9] Statista. (2023). *Percentage change on previous year of net income of the overall banking industry in the United States from 1st quarter 2007 to 1st quarter 2023*. Retrieved 11 16, 2023, from https://www.statista.com/statistics/1097062/us-bank-industry-income-growth-rate-per-quarter/

[10] Strupczewski, G. (2021). Defining cyber risk. *Safety Science, 135*.

