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

(RESEARCH ARTICLE)

Check for updates

# Cybersecurity Risks in US Financial Markets and the Implications for Investor Confidence and Market Stability

Chidozie Ebube Ebenmelu [1,*] and Bridget Nnenna Chukwu [2]

[1] *Department of Agricultural and Consumer Economics, University of Illinois, Urbana-Champaign, IL, USA.*
[2] *Department of Agribusiness and Applied Economics, North Dakota State University, Fargo, ND, USA.*

World Journal of Advanced Research and Reviews, 2025, 27(03), 1796-1808

Publication history: Received on 20 August 2025; revised on 25 September 2025; accepted on 29 September 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.3.3356

## Abstract

The growing digitalization of the U.S. financial markets has revealed the profound weaknesses to cybersecurity risks that question not only investor trust but also market stability. This paper looks at the impact of such breaches as ransomware, phishing, and malware on the resilience of a market and the view of systemic risk. With the mixed-method design, primary data collection was done by surveying investors, analysts, and regulators, and secondary data collection was done by case studies and regulatory reports. Results indicate that most of the respondents view the U.S. financial markets as very vulnerable, and breaches decrease investor confidence and result in restrictive investment behaviors. Cyber incidents have been broadly considered to have the capability to cause systemic shocks such as market volatility, reputation damage, and capital flight. Moreover, although respondents recognize the current regulatory frameworks, there is a doubt about their suitability for the modern, dynamic threats. The analysis concludes that cybersecurity governance is needed to minimize losses of money and also to ensure the stability and trustworthiness of the system. Greater collaboration between regulators, institutions, and technology providers is very important in ensuring resilience in the digital age.

**Keywords:** Cybersecurity Risks; Investor Confidence; Market Stability; Financial markets

## 1. Introduction

Digital technologies have changed the U.S. financial markets dramatically, altering the trading platforms, clearing systems, and payment networks. The combination of fintechs, algorithmic trading, and cloud-based infrastructure has increased market efficiency, increased the speed of transactions, and increased the involvement of investors. Nevertheless, there are also new vulnerabilities that the financial system has experienced due to these improvements since it has become increasingly dependent on interconnected digital networks prone to cyberattacks (Kopp, Kaffenberger & Wilson, 2017). Cybersecurity risks are also unique in that they have the capacity to propagate to institutions and sectors, inducing systemic instability. The financial sector is especially appealing to malicious actors due to the fundamental role it plays in the flow of funds, wealth management, and the overall world economy. Ransomware campaigns, phishing attacks, and state-sponsored intrusions demonstrate how vulnerable critical market infrastructure is and the increasing difficulty in providing resilience (Bouveret, 2018). The risk of cyber attack has been on the rise because of the growing complexity and rate of cyber attacks, and hence the desire to curb cyber attacks has also been on the rise, and this has attracted the attention of scholars, regulators, and industry players.

* Corresponding author: Chidozie Ebube Ebenmelu, Bridget Nnenna Chukwu

## 2. Review of Literature

The theoretical descriptions of cybersecurity and market stability can be described using the systemic risk theory, which says that the financial systems are highly interdependent, and therefore, the breakdown in one section can trigger an expansive impact on all other systems (Acharya et al., 2012). Cybersecurity cases are not an exception since the attacks are often targeted at central institutions that most times are clearinghouses, exchanges, and banks, whose functions add to the stability of the market in a significant way. The systemic risk theory is concerned with the predisposition to the propagation of the vulnerabilities of digital infrastructures across financial networks, making even small cyber infiltrations more significant (Kashyap & Wetherilt, 2020). Moreover, scholars have also pointed to the too-connected-to-fail dynamic, where an effective cyberattack against a significant institution does not just disrupt the market but also leaves behind the contagion effects that destabilize trust in the entire market (Bouveret, 2018). The contemporary financial markets are complicated, and, in addition to using digital platforms, they are susceptible to operational risks, which enhances the systemic nature of cyber threats. This theoretical contextualization brings out the reality that the problem of cybersecurity is not solely a technological problem but a stability problem, and no less attention should be paid to it than to traditional threats such as credit or liquidity shock (Cihak et al., 2020).

The empirical data of growing prevalence and economic effects of cyberattacks on financial markets, as well as the disruptive potential of cyberattacks, are evidenced. Research has shown that over the last decade, the number of cyber-attacks on banks and exchanges has been climbing at a very high rate as financial institutions start to rapidly digitalize (Laube and Böhme 2016). The discussion of specific cases, such as the 2017 ransomware of Ukrainian institutions that has captured global attention, shows that cyber threats can cross-contaminate both across borders and industries, the equity markets, payment systems, and investor trust (Anderson et al., 2012).

Financial regulators have identified these risks; the Bank for International Settlements (2018) noted that large-scale attacks can trigger systemic liquidity crunches and affect payment infrastructures, and that these risks have impacts on other asset classes. Similarly, empirical evidence in the U.S. highlights that post-cyber-attacks, abnormal negative stock performance is observed in publicly traded companies, particularly when the company itself is attacked and sensitive information or the business activity of the company is compromised (Kamiya et al., 2021). Interestingly, event studies show that such shocks not only impact immediately affected companies but also cascade to industry and market index participants, which are systemic in nature of cyber events (Kopp et al., 2017). This fact conclusively attests to the fact that cyber risks are not just threats at the firm level but also threats to the functioning of the markets.

According to the study on direct market disruption, the investor confidence and behavioral finance study will give details on the effects of the cybersecurity incidents on the perception and investment behavior of the markets. The traditional finance theory would suggest that the rational investor would respond to the news about cyber incidents by updating its risk assessment, but behavioral finance would suggest that biases and heuristics would increase the psychological impact of such shocks (Shiller, 2017).

As an example, when investors overreact to news of cyberattacks due to loss aversion and availability bias, equity markets would experience excessive volatility (Barberis, 2018). Investor sentiment studies also show that cyber-attacks not only undermine trust in the targeted companies but also the financial system as a whole, particularly when they point to an underlying weakness in digital infrastructures (Bongini et al., 2019). Confidence model accounts emphasize that financial markets are very sensitive to the feeling of security and reliability, and any shocks that undermine such feelings lead to capital flight, risk avoidance, and low liquidity in the market (Gai et al., 2020). The theoretical evidence also indicates that investors respond differently to the severity, visibility, and framing of cyber events. As an illustration, high-profile breaches that are frequently publicized in the media can cause disproportionate drops in stock prices, whereas less-publicized attacks can have muffled outcomes (Spatt and Zhang, 2022). These facts highlight the importance of behavioral dynamics in determining the relationship between cybersecurity events and financial stability outcomes.

Even after the advancement, there are still a lot of gaps in the literature on cybersecurity and market stability. A significant part of the available literature has focused on firm-specific implications of cyberattacks, including the impact on stock performance and image, but has not explored systemic aspects (Bouveret, 2018). Even though cyber incidents are central to financial stability, there is little empirical evidence regarding their impacts on interbank markets, payment systems, or derivative markets. Also, the geographical focus of research is mostly on developed economies, particularly the United States and Europe, and very few studies have been done on the emerging markets with less developed cybersecurity frameworks and institutional resilience (World Bank, 2020). The other gap is the connection between behavioral finance and systemic risk approaches; although both of these literatures recognize the significance of confidence and contagion, the interaction between investor psychology and systemic vulnerabilities in cyber crises is

not explicitly modeled (Kashyap and Wetherilt, 2020). Also, the fast rate of cyber threat development, such as the application of artificial intelligence and empowered attacks, as well as state-sponsored cyber warfare, provides researchers with moving targets, i.e., many empirical studies face the threat of becoming outdated unless constantly revised (Anderson et al., 2019). To fill these gaps, it is necessary to take interdisciplinary measures involving technical, financial, and psychological expertise that can help comprehend and reduce the multidimensional nexus of cybersecurity and financial market stability.

### 2.1. Current Emerging Issues in the Financial Market

The major risk of investor confidence and systemic stability is also caused by the increased cybersecurity attacks in the U.S. financial markets. A single attack on the market infrastructure or one of the large financial institutions can have far-reaching effects, including volatility, loss of liquidity, and reputation damage (Cornelli, Doerr, Gambacorta & Merrouche, 2020). Once the integrity of trading platforms or payment systems is impaired, it becomes hard to rattle investor confidence, which is the foundation of the functioning of capital markets. Behavioral finance research states that market participants tend to overreact to negative occurrences and may heighten the uncertainty, leading to capital flight (Biais, Bossaerts, and Spatt, 2021). Moreover, the dynamism of cyber threats is a challenge to the existing regulatory frameworks since the guidelines provided by various agencies, such as the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA), tend to be at a disadvantage to technological change. The problem, however, is that the complexity of cyber threats is growing, and the capacity of financial institutions and regulators to respond to the threats effectively is a gap that puts not only the trust of investors but the stability of the whole market under threat as well.

### 2.2. Research Objectives

This paper seeks to determine the effect of cybersecurity threats on investor confidence and market stability in the U.S. financial markets, as well as to determine the effectiveness of the existing regulatory responses. Specifically, the study attempts to determine whether cybersecurity breaches lower investor willingness to put money in, to what extent such breaches are perceived as capable of triggering systemic risks in the financial system, and whether regulatory measures, such as SEC cybersecurity disclosure regulations and FINRA guidelines, are thought to be sufficient to address such new threats. According to this, the main research questions are as follows: *Do cybersecurity breaches decrease investor confidence in U.S. financial markets? How far are such breaches perceived to be systemic risks? And do the existing regulatory frameworks seem sufficient to curtail the cybersecurity threats?*

## 3. Methodology

The research design adopted was a mixed-method research design because the authors aimed to investigate the problem of cybersecurity threats in the United States' financial markets and how they impact investor confidence and the stability of the markets. The quantitative section consists of a questionnaire containing 36 participants (investors, financial analysts, regulators, and market participants). A questionnaire with a structured format in terms of questions and both closed and open-ended was created to capture the perceptions of the risks of cybersecurity, the impact of the risks on the investor confidence, and perceptions of the regulatory responses. This is augmented by the qualitative aspect that will allow the respondents to provide exhaustive information on market resilience and policy needs.

Primary data is collected through the survey, and secondary data is collected through the assistance of published reports, regulatory releases, and case studies of cyber-attacks that occurred to financial institutions in the U.S. This two-dimensional approach provides a more valid outcome of the results as a result of quantitative tendencies and subjective data.

Such a purposive sampling technique is conducted in a manner that the participants should be equipped with the background knowledge required on financial markets and cybersecurity problems. The analysis of the data will be conducted through a combination of descriptive statistics (frequencies and percentages) in the case of quantitative responses and the thematic analysis in the case of qualitative inputs through a scatter bar chart representation. The informed consent, anonymity, and confidentiality of the information given by the respondents are ensured by ethical considerations.

### 3.1. Cybersecurity Risks in U.S. Financial Markets

The U.S. financial market operates in a highly digitalized environment, whereby there is a greater reliance on technological infrastructures, and this is an ideal environment where cybersecurity threats of all forms flourish. Malware, ransomware, phishing, and insider threats are the most intractable types of cyber threats that can destroy not

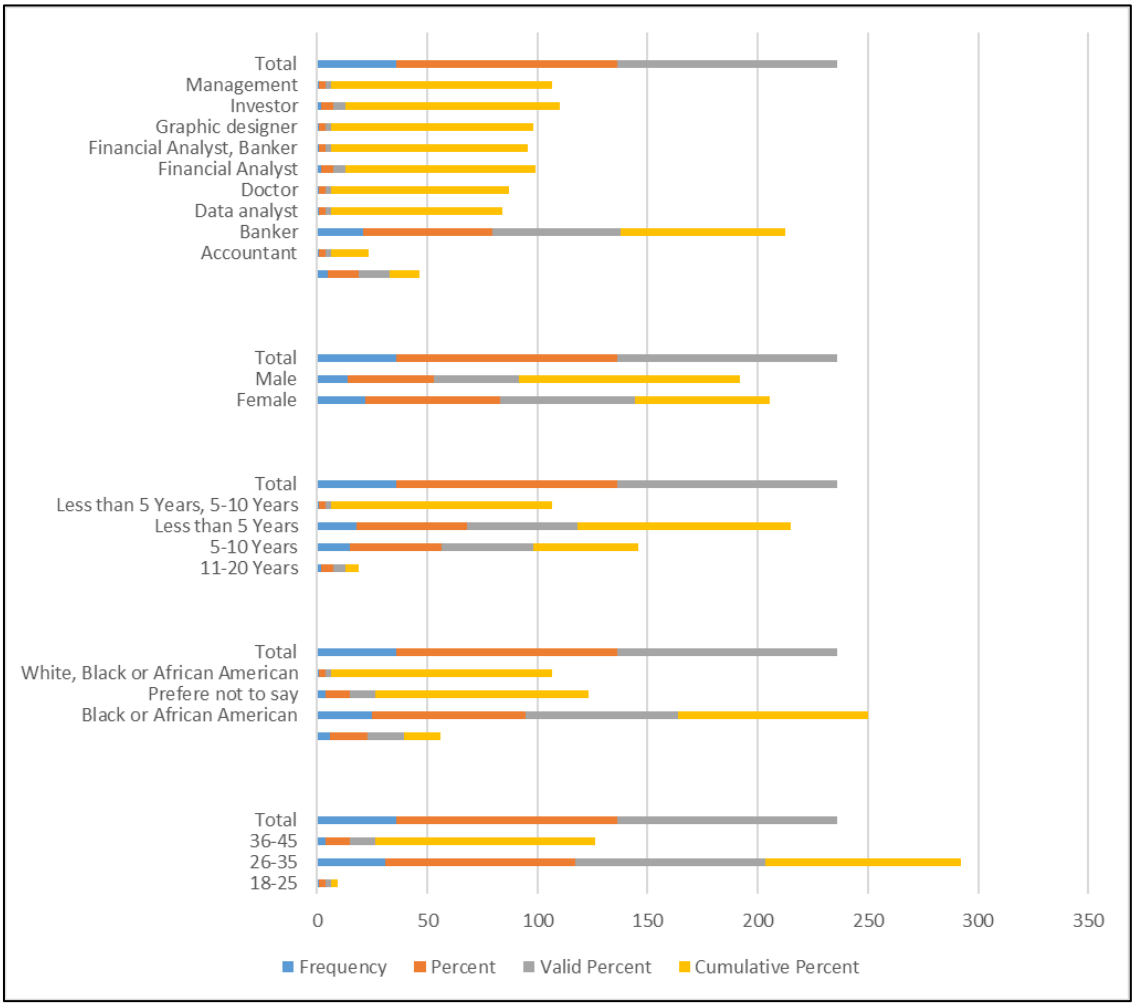
only the security of an institution but also the confidence of the people in financial stability. Malware or malicious software that is used to attack and destroy systems is also a persistent threat, as hackers keep upgrading their tools to avoid detection. Ransomware attacks, in which hackers encrypt systems and require payment to restore access, have especially increased in the financial industry as sensitive information is of high value and potentially costly financial losses can be incurred. Phishing attacks, which are usually based on a fake email or a malicious link that deceives employees into providing credentials, are still prevalent, and they take advantage of human weaknesses in security systems. The other major problem is insider threats, which include employees or contractors who are authorized to access the system and who may circumvent external controls and abuse their privileges to gain personal or malicious advantages (Anderson & Moore, 2012). All these threats highlight the fact that cybersecurity threats have advanced beyond technical nuisance to existential threats to the financial institutions, where breaches can create systemic damage to the markets within the United States.

The fact that some of the high-profile breaches portray the physical impact of these threats on the U.S. financial institutions and reflect the vulnerability of their infrastructure. The data breach of 2014 that involved JPMorgan Chase and personal data of over 76 million households and 7 million small businesses demonstrated how hackers can infiltrate one of the largest American banks and ruin the confidence in the market strength (Goldstein et al., 2014). In a similar manner, the case of the 2017 Equifax data breach that revealed personal data of 147 million Americans highlighted how one vulnerability of a credit reporting agency could disrupt consumer trust and institutional credibility and set ripple effects throughout the lending and investment markets (Federal Trade Commission, 2019). More recently, ransomware attacks such as the 2021 case of Colonial Pipeline (not necessarily a financial market attack, however) have shown how cyber disruption in any given industry can be extended into financial instability, which suggests that financial institutions are no less susceptible to advanced extortion attempts. The New York Department of Financial Services (2021) also indicated that there were many cases of cyberattacks on banks and insurers, where hackers exploited the poorly maintained systems of vendor management and the outdated authentication methodology. These case studies demonstrate that even well-resourced and regulated institutions are not immune, and each material violation highlights the fragility of the system as a whole, consumer protection, and the efficiency of the existing risk management frameworks.

The fact that these events are still occurring points to the general inefficiencies in the financial markets in the U.S., which are not just limited to the technical breakdowns in individual situations but also the structural risks in the entire framework. The interrelations between financial institutions through common technologies, cloud computing services, and third-party providers introduce the opportunities of one breach causing a catastrophe in the market. Financial markets can be disrupted by an attack on central clearinghouses, payment networks, or trading systems, which can prevent transactions, distort data integrity, or reduce investor confidence in the efficiency of the systems (Duffie, 2020).

The regulatory bodies, such as the Securities and Exchange Commission and the Federal Reserve, have once again reiterated that cybersecurity breaches could turn into the new liquidity crisis or credit shock, taking into account the fact that the contemporary financial markets rely on the digital infrastructure (Board of Governors of the Federal Reserve System, 2020). Furthermore, the problem of attribution and the sophistication of the state-sponsored cyber actors raises the risk, and the ill intent of the geopolitical interests can exploit the vulnerabilities to destabilize the U.S. economic security. This is worsened by the fact that the smaller financial institutions are not able to invest in cybersecurity as much as the larger organizations, leaving loopholes in the entire system that could be exploited by adversaries. In such a way, cyber threats in American financial markets cannot be seen as a one-time incident but rather a systemic weakness, which is constituted by the nature of digital finance with its technological reliance, human error, and international threat agents, providing a sense of systemic instability.

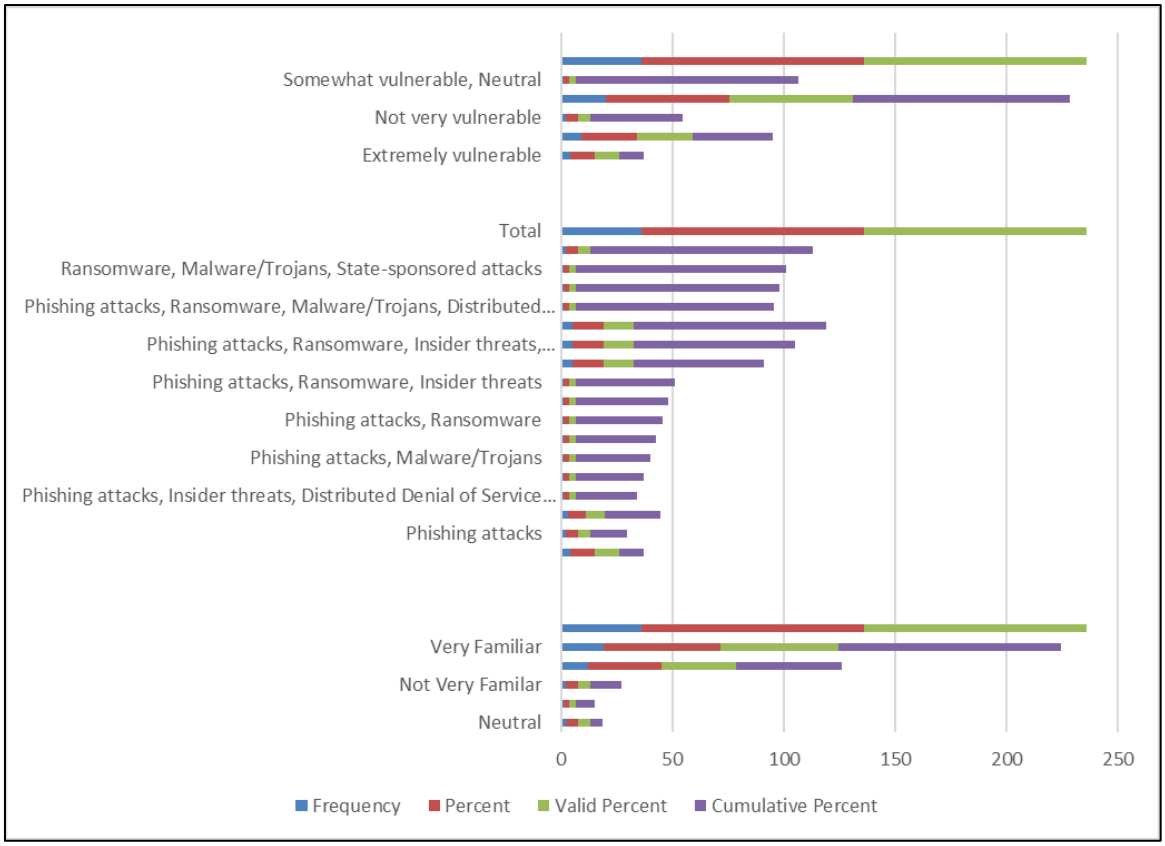
## 4. Discussion of Findings




Sources: Author's Field Work, 2025

**Figure 1** Scattered Chart indicating Demographics of Respondents

The provided chart represents the demographical data that was divided into several categories, including the following, profession (graphic designer, doctor, accountant), gender (male), years of experience (less than 5 years, 5-10 years, 11-20 years), age ranges (18-25 years old), and those who did not want to provide the answer to certain questions. Four measures are represented, including frequency, percent, valid percent, and cumulative percent, which give a detailed picture of the pattern of distribution. It is interesting to note that the highest cumulative percentage is recorded in the age group 18 to 25, which means that young respondents are the majority. Graphic designers and doctors have a relatively higher frequency of occupations than accountants in terms of professional distribution, indicating unequal distribution of the professions. The distribution of gender shows that there is a large number of males, and this is backed by fairly high frequencies and percentages. The years of experience indicate that the employees with less than 5 years of experience or between 5-10 years of experience in their respective disciplines constitute the majority of the respondents with those having over 11 years being lower in number and also being younger and with limited experience as a general sample. Interestingly, a low percentage did not provide demographic information to disclose which a bit influences valid percentages.

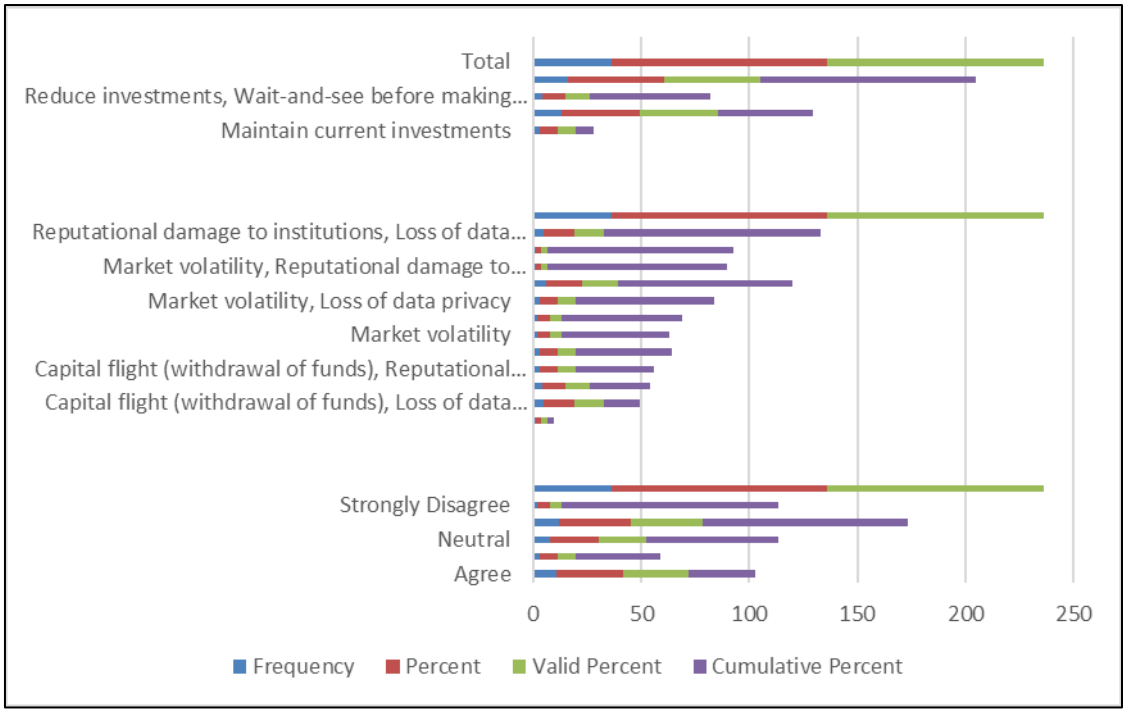



Sources: Author's Field Work, 2025

**Figure 2** Scattered Bar Chart of Awareness and Perception of Cyber Security Risk

The awareness and perception of cybersecurity risk chart is scattered, but it gives a clear understanding about the three research questions of the study. First, regarding the question of how cybersecurity breaches affect the confidence of investors in U.S. financial markets, the chart shows that the majority of the participants consider financial systems to be somewhat vulnerable and neutral, with smaller proportions of participants viewing financial systems as extremely vulnerable, which supports the argument that, although everyone is aware of the risk, the confidence in the resilience of financial systems is ambivalent, and more often than not, the participants mention ransomware, phishing, and malware, which substantiates the claim that breaches of the systems substantially undermine trust. Second, regarding the perceived severity of such breaches posing systemic risks, respondents listed a broad spectrum of threats, with phishing attacks, ransomware, and malware/Trojans getting the most frequent responses, followed by insider threats and distributed denial of service (DDoS), which supports the idea of systemic risk theory where a single major breach may spread across institutions and disrupt markets.

In terms of the sufficiency of existing regulatory frameworks, although the majority of the respondents indicated their level of awareness as very familiar or somewhat familiar with cyber threats, their concomitant feeling of high vulnerability indicates that despite being aware of the threats, they still did not have confidence that existing regulatory frameworks are adequate to address these emerging risks, which creates a disparity between threat awareness and perceived safeguards. In general, the chart demonstrates that participants are conscious and sensitive to cybersecurity risks, and they believe that they undermine investor confidence and systemic stability and are skeptical about the effectiveness of regulatory frameworks, which supports the research objectives of the study.

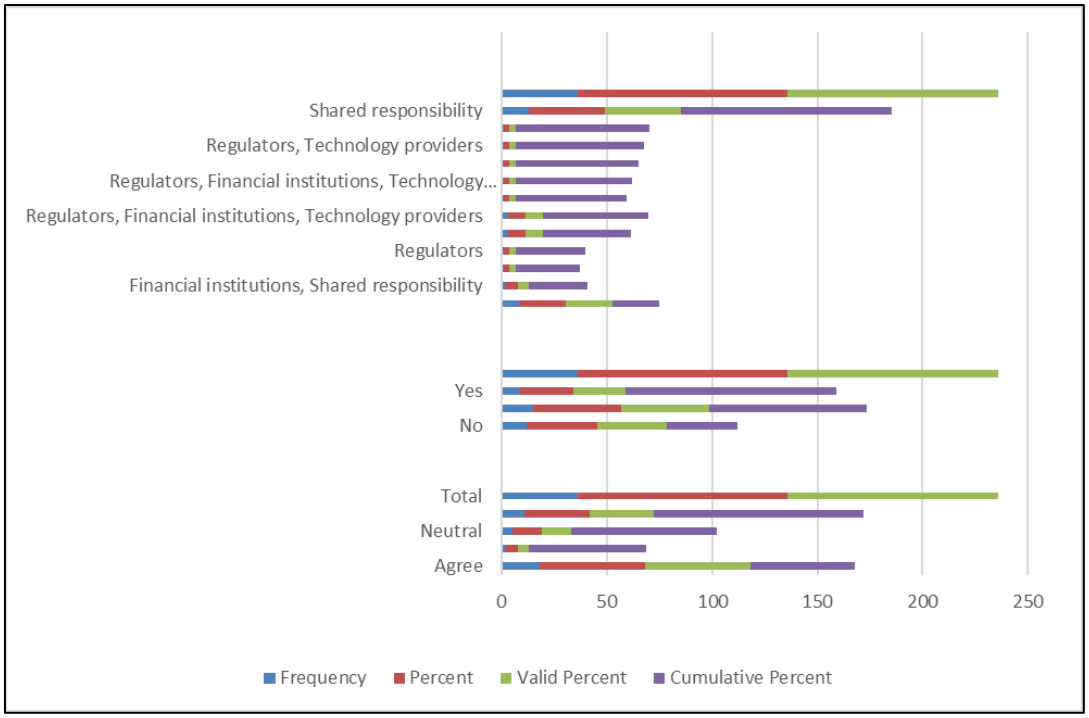



Source: Author's Field Work, 2025

**Figure 3** Stacked Bar Chart of the Impact of Cybersecurity Risk on Investor Confidence

The chart of investor reactions to cybersecurity risks is good evidence to the three research questions. First, regarding the issue of whether cybersecurity breaches cause a decline in investor confidence, the data prove that a large number of respondents would either decrease investments or wait-and-see, but fewer would keep investments, which proves that breaches make them more cautious and hesitant to take risks and invest, thus affecting confidence. Second, on the perceived scope of breaches to cause systemic risks, the consequences mentioned by the respondents include reputational damage to institutions, loss of data privacy, market volatility, and capital flight, all of which are not confined to individual firms but to the overall financial system; the frequent reference to capital flight and reputational crises is a sign of perceptions of systemic instability as was theorized by systemic risk theory.

Third, in the question of regulatory adequacy, the balance of views between agree, neutral, and strongly disagree indicates that, although some respondents are convinced that regulatory measures do exist, large proportions are skeptical of the same, and this implies a level of uncertainty of whether the current SEC and FINRA rules are just sufficient to adapt to the dynamic nature of threats. On the whole, the chart supports the fact that cybersecurity breaches reduce investor confidence, are viewed to have the ability to create systemic shocks, and reveal a disparity between regulatory provisions and investor anticipations, which directly justify the aims of the study.




Source: Authors Field Work, 2025

**Figure 4** Stacked Bar Chart of the Impact of Market Stability and Regulation

The market stability and regulation chart identifies the perception of the respondents with regard to the role and success of the key actors in ensuring that the U.S. financial markets are not subjected to cybersecurity attacks. This dominance of collective responsibility between regulators, financial institutions, and technology providers is a pointer to the shared realization that no single entity can ensure stability, instead, it will require a systemic robustness to organize actions. This is in accordance with the perception that cyber risks are systemic and can destroy the market unless it is managed collectively. As to the sufficiency of regulations, the responses are split: some of them believe that the current regulations facilitate the situation, and yet a significant portion of responses are neutral or even cynical, meaning that people do not know whether the SEC and FINRA systems are sufficient to adapt to the emerging threats. The cumulative percentages also highlight the fact that the respondents are aware of regulatory functions, but do not think that they can prevent systemic shocks on an equal measure.

These tendencies indicate that regardless of what regulatory frameworks are in place, market stability is regarded as weak and highly contingent on cooperation and is likely to have loopholes in oversight. By doing so, the chart demonstrates that the problem of cybersecurity threats continues to pose a threat to the stability of the market and indicates the failure of the current rules and regulations in guaranteeing the absolute trust of the investors and stability of the systems.

### 4.1. Integration of findings with existing literature

This research shows that breaches of cybersecurity impact negatively on investor trust, as it is consistent with previous research that demonstrates the ability of cyber events to undermine trust in financial systems. These charts show that the majority of respondents had lower intentions to invest or had a wait-and-see attitude following cybersecurity attacks, which supports the notion that trust in digital market structures is weak and responsive to risks. This aligns with behavioral finance views that indicate that investors are likely to overreact to negative happenings, which are usually caused by availability bias and loss aversion (Barberis, 2018; Shiller, 2017). The fact that the respondents recognized ransomware, phishing, and malware as typical threats is not new, since Laube and Bohme (2016) and Anderson et al. (2019) conducted their studies that revealed that such attacks were rapidly increasing and cross-sectoral. Moreover, the feeling that systemic shocks will have an effect is similar to the systemic risk theory, which assumes that a shock on a single segment of a connected financial system can rapidly diffuse to others (Acharya et al., 2012; Kashyap and Wetherilt, 2020). This highlights that the investor reluctance is not only due to firm-level weaknesses but rather because of the realization of systemic exposure, which increases the market-wide effects of cyber-attacks. It is important to also note that;

The statistics also reveal a high level of distrust towards the sufficiency of regulatory frameworks, despite the fact that the respondents were mostly familiar with cybersecurity threats. This helps to make the case that regulatory reactions like the SEC disclosure rules and FINRA regulations tend to follow technological advancements and the emerging threats (Cornelli et al., 2020; Board of Governors of the Federal Reserve System, 2020). Although there were respondents who admitted that regulations do exist, the most common skepticism about their effectiveness is indicative of gaps that have existed in the literature, with scholars stating that the majority of the current studies and policies address the risks of individual firms and do not fully tackle systemic risks (Bouveret, 2018; World Bank, 2020).

The results also indicate that stability was perceived by the respondents as a shared responsibility among the regulators, the financial institutions, and the technology providers. This focus on collective responsibility echoes Gai, Haldane, and Kapadia (2020), who believe that systemic stability is the key to financial stability in the digital age, as opposed to institutional protective measures. In addition, the ambivalent nature of the respondents regarding the sufficiency of existing regulations portrays the dynamic nature of regulations mentioned by Spatt and Zhang (2022), who believe that the regulatory provisions are usually responsive and not predictive, leaving the markets vulnerable to advanced and dynamic cyber threats.

The results on how investor attitudes towards systemic risks and market volatility are in line with empirical evidence that provides how cybersecurity events produce negative abnormal stock returns and reputational crises that extend beyond the directly affected companies (Kamiya et al., 2021; Bongini et al., 2019). The behavioral aspect of market instability, in which perceptions create more significant financial effects than actual ones, is highlighted by the common reference by respondents to capital flight and reputational damage. It aligns with the evidence provided by BIS (2018) and Duffie (2020) that underlines that a cyber-attack targeting payment systems or clearinghouses may rapidly spread into a larger liquidity effect and systemic crisis. The age of the respondents, who are mostly younger, especially those in the 18-25 age bracket and with less professional experience, might be the reason why the perception of vulnerability was high regardless of their knowledge of the regulations, as the new entrants to the market may be more sensitive to security and trust concerns. These results are consistent with the narrative economics approach described by Shiller (2017), which posits that tales of violations and insecurity drive sentiment and market action across the population. On the whole, the paper reinforces the current body of research by proving that cybersecurity threats negatively affect the investor confidence, increase the systemic risk perception, and expose the gaps in the regulatory frameworks, which is in line with the existing literature that agrees that effective governance and interdisciplinary approaches are the most important towards the stability of financial markets in the digital age of reliance.

## 5. Conclusion

This paper has revealed that cybersecurity threats have been a significant factor of investor confidence and market stability in the American financial markets. The investors, as shown by the findings, are extremely sensitive to cyber risks such as ransomware, phishing, and malware, where the majority of the respondents indicated that such risks decrease their intentions to invest or exercise a wait-and-watch approach. It agrees with the systemic risk theory and the behavioral finance perspectives, which emphasize that the interdependence of financial institutions and the psychology of investors enhances the disruptive nature of cyber incidents. The historical attacks, such as that of JPMorgan Chase and Equifax, have demonstrated empirically that even such well-developed institutions are vulnerable to attacks, and the reputational and operational losses that can be incurred as a result of such attacks can have cascading impacts on the broader financial system. In addition, uncertainty on the adequacy of the existing regulatory standards, such as those of the SEC and FINRA, creates a sense of disconnect between what regulators proclaim and what the market participants desire. Overall, the paper demonstrates that cybersecurity is not a technological issue, but a financial stability issue as well, and that the level of technological advancement, investor trust, and regulatory effectiveness is fragile.

### *Recommendations*

Based on these findings, a multi-stakeholder solution that seals the loopholes that lie between regulatory frameworks, institutional preparedness, and investor expectations should be employed to strengthen systemic resilience. Firstly, the regulatory bodies, i.e., SEC, FINRA, and the Federal Reserve, should be more active and proactive and should keep up with the development of cyber threats and their approaches should not be based on disclosure-based models. The tightening of the regulatory control should also be contemplated not only in big institutions but also in smaller financial institutions, which can be regarded as weak links in the system. Second, financial institutions should commit more resources to cybersecurity governance by prioritizing the organizational culture, training employees, and third-party risk management in order to realize that the vulnerability associated with people and vendors is no less important than technological vulnerability. Banks must endeavor to make sure that technological innovation and governance,

transparency, and ethical standards are all balanced to get maximum benefits (See: Bridget & Chidozie, 2025). Third, the enhanced cooperation among regulators, market operators, and technology providers needs to be institutionalized with the help of joint task forces, common intelligence systems, and unified cyber resilience standards. Lastly, investor confidence in the responses of institutional actors after the events should be restored and preserved through transparent communication strategies, since investors' perceptions are equally influenced by narratives and trust in the responses as much as by the financial losses suffered. Combined, these steps will contribute to making sure that investor confidence will be strengthened, systemic vulnerabilities will be minimized, and U.S. financial markets will be able to withstand the growing cybersecurity threats.

## Compliance with ethical standards

*Disclosure of conflict of interest*

No conflict of interest to be disclosed.

## References

[1] Acharya, V., Engle, R., & Richardson, M. (2012). Capital shortfall: A new approach to ranking and regulating systemic risks. American Economic Review, 102(3), 59–64.

[2] Anderson, R., & Moore, T. (2012). Information security: Where computer science, economics and psychology meet. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 378(2166), 20190167.

[3] Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2012). Measuring the cost of cybercrime. In The Economics of Information Security and Privacy (pp. 265–300). Springer.

[4] Bank for International Settlements. (2018). Cyber resilience: Range of practices. BIS.

[5] Barberis, N. (2018). Psychology-based models of asset prices and trading volume. In H. K. Baker & V. Ricciardi (Eds.), Behavioral finance (pp. 17–36). Wiley.

[6] Biais, B., Bossaerts, P., & Spatt, C. (2021). Market microstructure and financial markets stability. Journal of Financial Economics, 142(1), 1–20. https://doi.org/10.1016/j.jfineco.2021.02.003

[7] Board of Governors of the Federal Reserve System. (2020). Financial stability report. Washington, DC. https://www.federalreserve.gov/publications/2020-november-financial-stability-report.htm

[8] Bongini, P., Nieri, L., & Pelagatti, M. (2019). The effects of cyber-attacks on stock returns. Journal of Financial Stability, 40, 98–113. https://doi.org/10.1016/j.jfs.2018.11.002

[9] Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. IMF Working Paper 18/143.

[10] Bridget N. C. and Chidozie E. E. (2025). Artificial Intelligence and Fraud Detection in US Commercial Banks: Opportunities and Challenges. World Journal of Advanced Research and Reviews, 2025, 27(03), 1083-1091. Article DOI: https://doi.org/10.30574/wjarr.2025.27.3.3259.

[11] Cihak, M., Demirgüç-Kunt, A., & Peria, M. (2020). Financial stability monitoring. World Bank Policy Research Paper.

[12] Cihak, M., Demirgüç-Kunt, A., & Peria, M. (2020). Financial stability monitoring. World Bank Policy Research Paper. Washington, DC.

[13] Cornelli, G., Doerr, S., Gambacorta, L., & Merrouche, O. (2020). Cyber risk and financial stability: Evidence from the U.S. banking sector. Bank for International Settlements Working Papers, No. 865. https://www.bis.org/publ/work865.htm

[14] Duffie, D. (2020). Future of financial market infrastructures. Journal of Economic Perspectives, 34(3), 45–68. https://doi.org/10.1257/jep.34.3.45

[15] Federal Trade Commission. (2019). Equifax data breach settlement. Washington, DC. https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement

[16] Gai, P., Haldane, A., & Kapadia, S. (2020). Complexity, concentration and contagion. Journal of Monetary Economics, 125, 1–15. https://doi.org/10.1016/j.jmoneco.2020.01.004

[17] Goldstein, M., Hutton, E., & Stewart, J. (2014, September 26). JPMorgan hack exposed data of millions. The Wall Street Journal. https://www.wsj.com/articles/jp-morgan-discovers-hack-of-its-computer-systems-1412283377

[18] Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics, 139(2), 719–749. https://doi.org/10.1016/j.jfineco.2020.07.010

[19] Kashyap, A., & Wetherilt, A. (2020). Some principles for regulating systemic risk. Journal of Banking Regulation, 21(1), 1–17.

[20] Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. IMF Working Paper 17/185.

[21] Laube, S., & Böhme, R. (2016). The economics of mandatory security breach reporting to authorities. Journal of Cybersecurity, 2(1), 29–41. https://doi.org/10.1093/cybsec/tyv009

[22] New York Department of Financial Services. (2021). Cybersecurity in the financial services industry. New York: NYDFS.

[23] Shiller, R. J. (2017). Narrative economics. American Economic Review, 107(4), 967–1004. https://doi.org/10.1257/aer.107.4.967

[24] Spatt, C., & Zhang, H. (2022). Cyber risk and financial markets. Journal of Financial Economics, 146(2), 456–482. https://doi.org/10.1016/j.jfineco.2021.12.005

[25] World Bank. (2020). World Development Report 2020: Trading for development in the age of global value chains. World Bank.

## Appendices

*Survey Questionnaire*

**Title:** Cybersecurity Risks in U.S. Financial Markets and Investor Confidence

**Section A: Demographic Information**

- Age:
  - 18–25
  - 26–35
  - 36–45
  - 46–55
  - 56+
- Gender:
  - Male
  - Female
  - Prefer not to say
- Occupation/Role:
  - Investor
  - Financial analyst
  - Regulator
  - Banker
  - Other (please specify) _____
- Years of experience in financial markets:
  - Less than 5 years
  - 5–10 years
  - 11–20 years
  - 20+ years

*Section B: Awareness and Perceptions of Cybersecurity Risks*

- How familiar are you with cybersecurity risks in financial markets?

  - Very familiar
  - Somewhat familiar
  - Neutral
  - Not very familiar
  - Not familiar at all
- Which of the following cyber threats do you consider most serious for financial markets? (Tick all that apply)
  - Phishing attacks
  - Ransomware
  - Insider threats
  - Malware/Trojans
  - Distributed Denial of Service (DDoS)
  - State-sponsored attacks
- In your opinion, how vulnerable are U.S. financial markets to cyberattacks?
  - Extremely vulnerable
  - Somewhat vulnerable
  - Neutral
  - Not very vulnerable
  - Not vulnerable at all

*Section C: Impact on Investor Confidence*

- Do cybersecurity breaches reduce your confidence in investing in financial markets?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Which of the following consequences of breaches most affect investor confidence? (Select up to 2)
  - Market volatility
  - Capital flight (withdrawal of funds)
  - Reputational damage to institutions
  - Loss of data privacy
- After hearing about a major cyber breach, would you be likely to:
  - Reduce investments
  - Maintain current investments
  - Increase investments
  - Wait-and-see before making decisions

*Section D: Market Stability and Regulation*

- To what extent do you agree that cybersecurity breaches can trigger systemic risks in U.S. financial markets?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Do you think regulatory frameworks (e.g., SEC cybersecurity disclosure rules, FINRA guidelines) are sufficient to address cybersecurity threats?
  - Yes
  - No
  - Unsure
- In your view, who should bear the primary responsibility for ensuring cybersecurity in financial markets?
  - Regulators
  - Financial institutions
  - Technology providers
  - Investors themselves
  - Shared responsibility

*Section E: Open-Ended Questions*

- In your opinion, what additional measures should be taken to strengthen cybersecurity in U.S. financial markets?
- How can regulators, financial institutions, and investors collaborate better to maintain market stability against cyber threats?