Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Identifying Critical Cybersecurity Threats Impacting Financial Stability in Investment Firms: A Qualitative Risk Management Perspective

Qamarsultana Alad[1], James C Hyatt[2], and Rahul Azmeera[3]
[1] *Ph.D., Department of Information Technology, University of Cumberlands, Williamsburg, Kentucky, USA. University email: qalad26887@ucumberlands.edu*
[2] *Professor Department of Information Technology, University of Cumberlands, Williamsburg, Kentucky, USA. University email: james.hyatt@ucumberlands.edu.*
[3] *Independent researcher.* **E-mail:** *rahulazmeera@gmail.com. University of The Cumberlands*
Corresponding Author: Qamarsultana Alad **E-mail**: qalad26887@ucumberlands.edu

| ABSTRACT
Investment organizations now face greater cybersecurity risks as financial services become increasingly digitalized. Wherein the high-value transactions, sensitive client data, third-party platforms, and real-time operational systems are closely interconnected. The opinions of investment firm specialists on which specific risks pose the greatest threat to financial stability have not received as much attention as cyber risk, even though cyber risk has been thoroughly investigated using technological and quantitative approaches. This study used a qualitative case study to address the following research question: Which cybersecurity threats have the greatest impact on the financial stability of investment businesses? Semi-structured interviews with seven professionals in investment company settings were analyzed using thematic analysis informed by the Technology Acceptance Model, Risk Management Theory, and Contingency Theory. The findings demonstrate that the most serious threats are phishing, social engineering, third-party vendor risks, and the development of external threat vectors, as they have the potential to interfere with business operations, jeopardize data integrity, impair regulatory compliance, and erode investor confidence. The report argues that investment firms should view cybersecurity as a fundamental financial stability concern rather than a strictly technical function, and offers qualitative, theory-driven insights into cybersecurity threat prioritization.

| KEYWORDS
Cybersecurity, financial stability, investment firms, phishing, qualitative case study, risk management, third-party risk.

| ARTICLE INFORMATION
ACCEPTED: 01 June 2026 **PUBLISHED:** 29 July 2026 **DOI:** 10.32996/jcsts.2026.8.8.16

1. Introduction

The financial services sector has undergone a rapid digital transition driven by automation, cloud-based systems, mobile platforms, and integrated transaction infrastructure. Although these developments increase efficiency and market access, they also increase investment firms' susceptibility to cyberattacks [1], [2]. Investment firms are especially desirable targets because they handle sensitive customer data, manage portfolios, enable high-value transactions, and depend on continuous digital availability. Due to these circumstances, a cybersecurity incident may affect not just information systems but also operations, investor confidence, financial stability, and regulatory consequences [3], [4]. As a result, cybersecurity is no longer a minor technological concern. It is now a financial and organizational risk that interacts with human behavior, technological adoption, risk management, governance, and regulatory compliance [5], [6]. Earlier studies have highlighted major financial issues, such as data breaches, ransomware, phishing, insider risk, third-party vulnerabilities, and advanced persistent threats [7], [8]. Nevertheless, a more comprehensive qualitative examination of the financial stability implications of these threats in investment business settings is required, as the severity of a cyber threat is determined by technological exposure and by how experts understand, prioritize, and respond to risk.

Previous research has frequently used quantitative models, breach-cost analysis, technical protections, and regulatory frameworks to address cybersecurity. The lived and professional perspectives of employees of investment firms that address cybersecurity concerns in actual organizational contexts constitute a significant gap left by this research, despite its value. Because qualitative research captures how organizations perceive vulnerability, how threat categories relate to financial implications, and how threats are perceived, it can help close this gap [21], [24].

Only the threat-identification aspect of the larger investigation is the focus of this paper. It asks: Which cybersecurity risks have the greatest impact on the financial stability of investment firms? The study makes three contributions. It begins by identifying the cyber threats that experts at investment firms believe have the greatest impact on financial stability. Second, it links these risks to the Technology Acceptance Model, Risk Management Theory, and Contingency Theory. Third, it has useful implications for investment businesses looking to enhance threat prioritization, vendor supervision, staff knowledge, and cybersecurity governance.

1.1 Research Question

Which cybersecurity threats have the most significant effects on investment firms' financial stability?

2. Literature Review

2.1 Cybersecurity Threats in Financial Organizations

As financial institutions increasingly depend on interconnected digital platforms, cybersecurity risks in financial companies have become more frequent and complex [1] [3]. Because they operate within a broader financial ecosystem that connects client accounts, trading platforms, vendor systems, cloud services, internal users, and regulatory reporting procedures, investment firms are vulnerable to cyber risk. Consequently, technical, operational, and financial sectors may be affected by cybersecurity incidents [6], [18].

Since the systems are encrypted, vital activities are disrupted, and there is pressure to secure a quick financial recovery, ransomware remains one of the most disruptive cyberthreats [8]. Operational downtime is particularly harmful to financial institutions since delays in transaction processing, client service, or portfolio management can affect both revenue and trust. Costs for recovery, legal assessment, business disruption, and reputational repair can be considerable even when ransom payments are not made.

Because they exploit human judgment rather than technological flaws, phishing and social engineering pose major risks. Phishing employs misleading messages to install malicious software, steal credentials, or persuade users to engage in risky activities [5], [14]. By influencing urgency, authority, familiarity, or trust, social engineering increases this danger. Employees are frequently the means by which attackers get beyond technical safeguards, according to human-factor research [4], [13]. Investment businesses may be able to access confidential systems, customer information, or internal processes with just one compromised credential.

Insider attacks make cybersecurity much more difficult because they might be deliberate or inadvertent. Employees, contractors, or privileged users may misuse access, mishandle data, ignore security precautions, or unintentionally permit breaches [4], [16]. Insider risk is especially significant in financial firms, as customer trust and regulatory compliance depend heavily on secrecy, integrity, and access controls. As investment firms rely more and more on vendors for cloud hosting, analytics, cybersecurity tools, transaction services, data management, and compliance support, third-party and supply chain risks have become increasingly important. Vulnerabilities that are not directly under the company's control may be introduced by external sources. Because flaws in one vendor environment may impact several financial institutions, supply-chain risk is a systemic concern [6], [18].

2.2 Cybersecurity and Financial Stability

The ability of investment firms to sustain dependable operations, secure assets, maintain data integrity, adhere to rules, and maintain investor trust in the face of internal and external upheavals is referred to in this study as financial stability. Cyber risks in both direct and indirect ways impact financial stability. Direct routes include things like service interruptions, remediation

expenses, fraud losses, incident response fees, and recovery delays. Reputational harm, regulatory scrutiny, client mistrust, liquidity pressure, and diminished market confidence are examples of indirect channels [17], [18].

The importance of cybersecurity risk is increased by financial institutions' interconnectivity. Clients, data suppliers, payment systems, related companies, and counterparties may all be impacted by a cyber event that starts in one business [9]. Because investment firms operate in time-sensitive marketplaces where accuracy, consistency, and confidence are critical, this systemic feature is crucial. Therefore, cybersecurity should be included in enterprise risk management rather than only information technology [12], [20].

Financial businesses must invest in cybersecurity while balancing costs, usability, regulatory pressure, and operational efficiency, which poses a governance challenge, according to the literature [20], [22]. Overdependence on technological controls might overlook differences in organizational context, vendor exposure, and human conduct. The need for a qualitative study into how professionals recognize the risks that most immediately threaten financial stability is made clear by this discrepancy.

3. Theoretical Framework

Three complementary theories serve as the foundation for this paper: the Technology Acceptance Model (TAM), Contingency Theory, and Risk Management Theory. When combined, these frameworks facilitate the examination of financial, organizational, and behavioral risks associated with cybersecurity threats. Systematic risk identification, evaluation, prioritizing, mitigation, and monitoring are highlighted by risk management theory [12], [20]. The idea in this study explains why investment businesses need to determine which cyber threats pose the greatest risk to financial stability. The initial phase in significant risk prioritization is recognizing threats. Failing to identify the most critical threats can jeopardize the effective use of cybersecurity resources or leave companies unprepared for significant incidents.

According to contingency theory, organizational responses ought to be appropriate to the environment in which they function [22], [23]. Not all investment organizations face the same level of cybersecurity risk. The way cybersecurity threats are perceived and addressed is influenced by several factors, including firm size, digital maturity, regulatory exposure, vendor dependence, budget, and organizational culture. Therefore, a context-dependent rather than one-size-fits-all understanding of cybersecurity risk is supported by contingency theory.

Technology adoption and use are influenced by perceived utility, perceived ease of use, and user attitudes, as explained by TAM [25]. Since many of the risks found in this study rely on human behavior, TAM is pertinent to cybersecurity. Employee comprehension, trust, and appropriate use of cybersecurity tools and procedures influence phishing, social engineering, and insider errors. As a result, the framework helps link user behavior to financial risk and threat exposure.

4. Methodology

The cybersecurity risks thought to have the greatest impact on investment businesses' financial stability were investigated using a qualitative case study design. Because the research topic focused on professional opinions, organizational experience, and contextual interpretation rather than statistical measurement, a qualitative approach was appropriate [21], [24]. The larger dissertation study comprised seven participants. Professionals with expertise in cybersecurity, risk management, technology systems, or operational procedures in investment company settings, such as project managers, system analysts, and IT developers, were among the participants. To find people with relevant expertise, purposeful sampling was employed [19].

Data was collected through semi-structured interviews. Participants consistently explained threat experiences, organizational vulnerabilities, and perceived financial stability implications in their own words throughout the interviews. Thematic analysis criteria, such as coding, pattern recognition, theme development, and interpretation, were adhered to in the analysis [15], [24]. The cybersecurity threat landscape, including phishing attacks, social engineering, third-party vendor concerns, and evolving external threat vectors, was the main theme of the research question.

5. Findings

Participants viewed cybersecurity concerns as ongoing, external, and persistent hazards to investment firms, according to the study's research question. The main risks identified are changing external threat vectors, social engineering, phishing scams, and third-party provider vulnerabilities. The research question is consistent with these results.

Table 1. Critical cybersecurity threats and financial stability impact

Threat	Evidence from interviews	Financial stability impact
Phishing	Daily phishing attempts; a single employee's click can grant access.	Credential compromise; system and client-service disruption.
Social engineering	Attackers use urgency, authority, and internal-looking messages.	Bypassed controls; unauthorized access; weakened trust.
Third-party vendor risk	Reliance on external systems with limited visibility.	Supply-chain exposure; operational and data-risk spillover.
Evolving external vectors	Persistent adaptive threats, including ransomware and data breaches.	Incident response costs, regulatory and reputational exposure.

5.1 Phishing Attacks

The most often mentioned threat in the research question results was phishing. Because phishing directly targets employees and can provide an entry point into company systems, participants assessed it as a persistent and practical threat. Participant 4 said, "We encounter phishing emails nearly daily, and if just one individual click, it can pave the way for cyber attackers." This quotation demonstrates that participants viewed phishing as a persistent operational threat rather than an infrequent annoyance.

Phishing's impact on financial stability stems from its capacity to convert human error into system risk. Credential theft, illegal access, data compromise, or disruption of client-related processes are all possible outcomes of a successful phishing attempt. According to participant 1, these kinds of situations could result in "major disruption to our systems and client interactions." This result is consistent with studies indicating that phishing is one of the most prevalent and dangerous cyber threats businesses must address [2], [5], and [14].

5.2 Social Engineering

One similar but different threat that has emerged is social engineering. In general, social engineering entails psychological manipulation, whereas phishing frequently refers to misleading messages. Attackers "play on urgency or authority," according to participant 6, which might even cause experienced workers to make mistakes. This research further supports the significance of human susceptibility in cybersecurity outcomes.

According to participant 2, some attempts "appear to be coming from someone inside the company, which makes them more convincing." For investment organizations, this is crucial, since internal communication might circumvent common suspicion and increase the risk of risky behavior. Social engineering can compromise the integrity of internal procedures, lead to illegal activities, and erode confidence in communication networks from a financial stability perspective. The result is consistent with human-factor research, which highlights that behavior-based hazards cannot be completely prevented by technical controls alone [4], [13].

5.3 Third-Party Vendor Risk

Risk from third-party vendors was another significant issue. Investment firms rely on outside platforms, vendors, and service providers, but they don't necessarily have complete visibility into those providers' security procedures, participants stressed. Participant 7 said, "Any breach on their end immediately impacts us, because we rely heavily on external systems." This suggests that direct company exposure may result from vendor exposure.

Participant 3 also stated, "We have to trust that our vendors are handling it properly because we don't always have full insight into their security measures." This result aligns with research demonstrating that reliance on third parties can increase systemic cyber risk [6], [18], and with the NIST Cybersecurity Framework's emphasis on supply-chain risk management [3]. Even when the initial breach occurs outside the company, third-party incidents can disrupt services, compromise shared data, create legal requirements, or undermine client confidence, all of which affect financial stability [11].

5.4 Evolving External Threat Vectors

Additionally, participants characterized the overall cybersecurity threat landscape as dynamic and enduring. Despite being the most well-defined research question threats, ransomware, data breaches, and sophisticated attacks were among the many

external threat vectors. Ransomware literature indicates that these incidents can incur significant recovery costs and quickly disrupt operations [8].

According to the research, investment firms view cybersecurity as a dynamic risk environment rather than a static collection of dangers. This is important because being prepared for evolving risks is essential to financial stability. When attackers modify tactics or exploit new technologies, remote access, cloud dependencies, or supplier vulnerabilities, controls that target a single type of attack might not be sufficient [7], [10].

6. Discussion

6.1 Interpretation of Findings

The results show that cybersecurity risks that combine high likelihood, human vulnerability, and operational consequence are the most serious dangers to the financial stability of investment organizations. Phishing was noteworthy due to its frequency and the fact that it only takes one successful staff action to spread awareness. Social engineering was significant because it exploits trust, authority, or urgency to bypass technical protections. Because it expands the firm's attack surface outside organizational boundaries, third-party vendor risk is substantial. Because they reflect the dynamic nature of cyber risk, evolving external vectors were significant.

These findings support Risk Management Theory by demonstrating that threat identification is foundational to financial stability. Without determining which cyberthreats are most critical to business continuity, data integrity, compliance, and investor trust, investment firms cannot effectively prioritize measures [12], [20]. Because contextual factors, including vendor dependence, staff knowledge, digital development, and regulatory duties, shape organizations' vulnerability, the findings also corroborate Contingency Theory [22], [23]. Because phishing and social engineering demonstrate how users' behavior, comprehension, and acceptance of security procedures affect the effectiveness of technology, TAM is represented in the results [25].

The results also demonstrate the various ways in which cyber dangers pose a threat to financial stability. System interruption, transaction delays, and poor client communication are examples of operational mechanisms. Loss of confidence following a perceived breach of information security is one of the reputational processes. Compliance investigations, reporting requirements, and potential fines are examples of regulatory procedures. Recovery costs, remediation costs, lost revenue, and indirect harm to business value are examples of financial mechanisms [17], [20].

6.2 Implications for Practice

The research suggests that investment businesses treat social engineering and phishing as strategic threats rather than as widespread public awareness issues. Training should be continuous, scenario-based, and related to actual business operations. Moreover, firms should have reporting mechanisms in place that allow workers to report dubious assertions without fear of retaliation.

Third-party risk management should receive more attention from governance. Vendor evaluations should include cybersecurity controls, incident response procedures, data handling requirements, and monitoring capabilities. As participants stated they had limited visibility into vendors' security procedures, companies should strengthen contractual requirements, expand audit rights, and maintain ongoing third-party risk assessments.

Cybersecurity measures should be incorporated into financial risk reporting at the business level. Information on phishing exposure, vendor risk posture, incident response preparedness, and potential financial implications should be provided to boards and top executives, along with details on technical controls. This would enhance decision-making by aligning cybersecurity with enterprise risk management.

7. Limitations

There are several limitations to this study. First, the sample may include only seven participants. Although this allows for in-depth analysis and is suitable for qualitative research, it restricts statistical generalizability [19], [21]. Second, the study used self-reported participant perceptions, which could be impacted by company culture, role, memory, or confidentiality restrictions. Third, transferability to other financial institutions, such as commercial banks, insurance companies, or credit unions, is constrained by the emphasis on investment businesses. Lastly, because cybersecurity threats are constantly evolving, the threat environment described in this study may change as attackers adopt new tools and techniques.

8. Future Scope

This study should be expanded upon in future research by incorporating larger, more varied samples across various financial sectors. The association between particular hazard categories and quantifiable financial effects, including recovery costs, downtime, regulatory fees, and client attrition, could be examined through quantitative research. Comparative research could examine how perceptions of threat severity vary across small, mid-sized, and large investment enterprises. Future research should also examine emerging concerns, including deepfake-enabled fraud, automated social engineering, AI-enabled phishing, cloud misconfiguration, and advanced persistent threats [11]. Given the significance of third-party risk, further research should examine how supply-chain monitoring, contractual controls, and vendor governance affect investment firms' financial stability.

9. Conclusion

This paper investigated the cybersecurity risks deemed most important to the financial stability of investment organizations. Because they can interfere with operations, jeopardize data integrity, erode compliance, and undermine investor trust, the results demonstrate that phishing, social engineering, third-party vendor risks, and developing external threat vectors are major concerns. The study shows that cybersecurity risk in investment organizations involves financial, organizational, and behavioral factors rather than just technological ones. The study emphasizes the need for integrated cybersecurity solutions that address vendor exposure, human behavior, and adaptive threat environments, drawing on Risk Management Theory, Contingency Theory, and TAM. As a fundamental corporate risk management function, cybersecurity should be given top priority by investment firms, and controls should be constantly adjusted to reflect the changing threat landscape.

Funding: No external funding was received for this research.
Conflicts of Interest: The author declares no conflict of interest.
ORCID iD 0009-0006-0525-9515
Publisher's Note: **Acknowledgments**
The author thanks academic peers and enterprise professionals for valuable discussions and feedback

References

[1] F. Cremer, B. Sheehan, M. Fortmann, A. N. Kia, M. Mullins, F. Murphy, and S. Materne, "Cyber risk and cybersecurity: A systematic review of data availability," The Geneva Papers on Risk and Insurance - Issues and Practice, vol. 47, no. 3, pp. 698-736, 2022, doi: 10.1057/s41288-022-00266-6.

[2] A. Chidukwani, S. Zander, and P. Koutsakis, "A survey on the cybersecurity of small-to-medium businesses: Challenges, research focus, and recommendations," IEEE Access, vol. 10, pp. 85701-85719, 2022, doi: 10.1109/ACCESS.2022.3197899.

[3] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD, USA: NIST, 2018, doi: 10.6028/NIST.CSWP.04162018.

[4] L. Hadlington, "The human factor in cybersecurity: Exploring the accidental insider," in Research Anthology on Artificial Intelligence Applications in Security. Hershey, PA, USA: IGI Global, 2021, pp. 1960-1977.

[5] M. M. Ali and N. F. Mohd Zaharon, "Phishing - A cyber fraud: The types, implications and governance," International Journal of Educational Reform, vol. 33, no. 1, pp. 101-121, 2024, doi: 10.1177/10567879221082966.

[6] R. Walton, D. J. Wheeler, and G. Zhang, "Cybersecurity frameworks and emerging risks in financial organizations," Journal of Cybersecurity and Risk Management, vol. 8, no. 2, pp. 44-61, 2020.

[7] A. K. Mishra, A. K. Vishwakarma, and A. K. Patel, "Smart systems and cybersecurity risks in digital infrastructures," Smart Engineering Technology and Management, pp. 304-318, 2024.

[8] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, "Ransomware: Recent advances, analysis, challenges, and future research directions," Computers & Security, vol. 111, Art. no. 102490, 2021, doi: 10.1016/j.cose.2021.102490.

[9] M. Uddin, M. H. Ali, and M. A. Hassan, "Cybersecurity hazards and financial system vulnerability: A synthesis of emerging risks," International Journal of Financial Studies, vol. 8, no. 4, pp. 1-18, 2020.

[10] D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity: A comprehensive survey," The Journal of Defense Modeling and Simulation, vol. 19, no. 1, pp. 57-106, 2022, doi: 10.1177/1548512920951275.

[11] B. Bala, M. Prasad, and R. Kumar, "AI techniques for IoT-based DDoS attack detection: A systematic literature review," Computer Networks, vol. 236, Art. no. 110033, 2024, doi: 10.1016/j.comnet.2023.110033.

[12] P. Hopkin, Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management, 4th ed. London, U.K.: Kogan Page, 2018.

[13] J. Jeong, J. Mihelcic, G. Oliver, and C. Rudolph, "Towards an improved understanding of human factors in cybersecurity," in Proc. IEEE 5th Int. Conf. Collaboration and Internet Computing (CIC), 2019, pp. 338-345, doi: 10.1109/CIC48465.2019.00047.

[14] A. Pollini, A. Callari, A. Tedeschi, D. Ruscio, L. Save, F. Chiarugi, and R. Guerri, "Leveraging human factors in cybersecurity: An integrated methodological approach," Cognition, Technology & Work, vol. 24, pp. 371-390, 2022.

[15] V. Clarke, V. Braun, and N. Hayfield, "Thematic analysis," in Qualitative Psychology: A Practical Guide to Research Methods, 3rd ed., J. A. Smith, Ed. London, U.K.: Sage, 2015, pp. 222-248.

[16] M. G. Gelles, K. Mitchell, S. D. Hart, and L. S. Guy, "Top 10 considerations for building an insider threat mitigation program," Journal of Threat Assessment and Management, vol. 2, no. 3-4, pp. 255-257, 2015, doi: 10.1037/tam0000059.

[17] W. Steingartner, D. Galinec, and K. Kozina, "Threat defense: Cyber deception approach and education for resilience in hybrid threats model," Symmetry, vol. 13, no. 4, Art. no. 597, 2021.

[18] F. Gomez Marmol, M. Gil Perez, and G. Martinez Perez, "I don't trust ICT: Research challenges in cyber security," in Proc. IFIP Int. Conf. Trust Management, 2016, pp. 129-136.

[19] L. A. Palinkas, S. M. Horwitz, C. A. Green, J. P. Wisdom, N. Duan, and K. Hoagwood, "Purposeful sampling for qualitative data collection and analysis in mixed method implementation research," Administration and Policy in Mental Health and Mental Health Services Research, vol. 42, no. 5, pp. 533-544, 2015, doi: 10.1007/s10488-013-0528-y.

[20] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, "Increasing cybersecurity investments in private sector firms," Journal of Cybersecurity, vol. 1, no. 1, pp. 3-17, 2015, doi: 10.1093/cybsec/tyv011.

[21] J. W. Creswell and C. N. Poth, Qualitative Inquiry and Research Design: Choosing Among Five Approaches. Thousand Oaks, CA, USA: Sage, 2016.

[22] D. Otley, "The contingency theory of management accounting and control: 1980-2014," Management Accounting Research, vol. 31, pp. 45-62, 2016.

[23] H. Li, W. G. No, and T. Wang, "SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors," International Journal of Accounting Information Systems, vol. 31, pp. 1-13, 2018, doi: 10.1016/j.accinf.2018.06.003.

[24] L. S. Nowell, J. M. Norris, D. E. White, and N. J. Moules, "Thematic analysis: Striving to meet the trustworthiness criteria," International Journal of Qualitative Methods, vol. 16, no. 1, pp. 1-13, 2017, doi: 10.1177/1609406917733847.

[25] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," MIS Quarterly, vol. 13, no. 3, pp. 319-340, 1989, doi: 10.2307/249008.