Risk Management and Investment
Volume 4, Number 2, 2025

Cyber Risk Management and Its Impact on Investment Performance

Syakira Gavrila Haerus[1*]

[1] Telkom University, Bandung, Indonesia

Abstract

Article history:
Received: August 24, 2025
Revised: September 8, 2025
Accepted: October 13, 2025
Published: December 30, 2025

Keywords:
Assurance, Cyber Risk, Disclosure, Expected Returns, Investment Performance.

Identifier:
Zera Open
Page: 112-126
https://zeraopen.com/journal/rmi

Cyber risk is a financially material source of uncertainty that can reshape expected cash flows, downside tail risk, and investor confidence. This systematic literature review asks how cyber risk and cyber risk management influence investment performance, through which mechanisms, and when effects differ by context and measurement. Using peer-reviewed studies published from 2019 to 2024, the review synthesizes evidence across finance, accounting, and information systems. Findings show that cyber risk is reflected not only in breach-driven valuation shocks but also in latent exposure that affects risk premia and tail outcomes such as crash risk. The article discusses results through a mechanism-based lens linking governance and investment discipline, response reliability, disclosure credibility, and contracting spillovers to investment-relevant outcomes. Overall, cyber risk management is most performance-relevant when it lowers expected loss severity, strengthens credible assurance signals, and improves disclosure quality that reduces information asymmetry and ambiguity. Variation is explained by investor attention, industry digital intensity, inter-firm dependence, and proxy choice.

*Corresponding author:
(Syakira Gavrila Haerus)

1. Introduction

Cyber risk has moved from being a narrow IT problem to a financially material source of uncertainty that can reshape expected cash flows, downside tail risk, and investor confidence. For listed firms, cyber incidents can trigger immediate valuation losses, while the anticipation of future attacks can be incorporated into risk premia and required returns. Recent finance research supports this broader framing by showing that cybersecurity risk exposure can be priced in the cross-section of stock returns, yet the same exposure can become a liability when cybersecurity risk in the environment intensifies and investors rotate toward resilience (Florackis et al., 2023). These dynamics make cyber risk management relevant not only for operational continuity, but also for investment performance outcomes that matter to shareholders, lenders, and portfolio managers.

The link between cyber risk management and investment performance is multi-channel. At the firm level, cybersecurity practices influence the likelihood and severity of breaches, the speed and credibility of disclosure, and the magnitude of reputational and regulatory costs. Market evidence indicates that breach disclosures can elevate crash risk, reflecting amplified investor concerns about vulnerability and uncertainty, particularly when governance and information frictions are present (Cao et al., 2024). Regulation can also reshape these outcomes by changing disclosure incentives and information quality. For example, tighter disclosure deadlines can accelerate reporting but may reduce the detail available at the time of disclosure, with observable implications for how investors react to delays versus more complete disclosures (Ashraf et al., 2022).

Cyber risk management itself is not a single practice, but a portfolio of governance, controls, assurance, and investment decisions that vary in maturity and effectiveness. Managerial and organizational research emphasizes frameworks that align technical safeguards with enterprise risk management and cost analysis, clarifying how cyber investments can be evaluated alongside other capital allocation choices (Lee, 2021). Leadership and human capital also shape cyber outcomes: executive IT expertise has been associated with differences in reported security breaches, indicating that top management capabilities can influence cyber prevention, detection, and incident governance (Haislip et al., 2021). Assurance mechanisms matter as well. Internal audit effectiveness in cybersecurity has been operationalized and linked to stronger cybersecurity risk management maturity, suggesting that monitoring and control processes can be an important capability even when breach prevention remains imperfect (Slapničar et al., 2022). Disclosure practices add another layer because they shape information asymmetry and investor learning. Longitudinal evidence on public firms' cybersecurity risk disclosures shows systematic shifts in disclosure content and language, reinforcing the idea that markets increasingly interpret cyber risk narratives as part of fundamental risk assessment (Gao et al., 2020).

At the same time, cyber risk can propagate beyond the breached firm through economic linkages, altering perceived risk in supply chains and affecting third-party assessments of reliability. Evidence that customer breaches can spill over into suppliers' audit fees highlights how cyber events can change the broader contracting environment and the cost structure surrounding financial reporting and monitoring

(Zhang & Smith, 2023). Breaches can also surface as internal control consequences, linking cyber events to financial reporting processes and control assessments that investors may treat as signals of broader governance quality (Zhou & Huang, 2024). Because these channels operate simultaneously, empirical findings can appear fragmented across disciplines: some studies focus on incident-driven market reactions, others on priced risk exposure, and others on governance and assurance mechanisms that shape resilience and transparency. Strategic timing of breach announcements further complicates inference by attenuating observed market reactions when attention is distracted, implying that average effects can mask meaningful heterogeneity (Foerderer & Schuetz, 2022).

This study addresses that fragmentation through a systematic literature review of peer-reviewed evidence on cyber risk management and its impact on investment performance. The review synthesizes how cyber risk management capabilities influence investment outcomes across multiple levels of analysis, including firm valuation and stock performance, risk premia and tail risk, disclosure credibility and information asymmetry, and indirect spillovers through auditors, partners, and supply networks. By integrating insights from finance, accounting, information systems, and risk management, the review develops a structured map of mechanisms and boundary conditions that explain when cyber risk management strengthens investment performance and when it mainly repositions risk across stakeholders. The expected contribution is a clearer causal logic for researchers and a decision-oriented synthesis for practitioners, supporting more coherent measurement

choices, more testable propositions, and more investment-relevant interpretations of cyber resilience.

2. Literature Review

Cyber risk is increasingly conceptualized as an investment-relevant source of uncertainty rather than an isolated operational issue. Beyond the immediate costs of incidents, scholarship emphasizes that cyber exposure can affect expected cash flows and the distribution of returns by elevating downside tail risk and amplifying uncertainty about future disruptions. This is consistent with asset pricing evidence that cybersecurity risk exposure can be priced in the cross-section of stock returns, implying that investors incorporate cyber vulnerability into required returns and portfolio allocation decisions (Florackis et al., 2023). In this framing, cyber risk management becomes relevant not only as loss prevention, but as a capability that can alter risk premia, resilience perceptions, and the credibility of firm value over time.

A recurring mechanism linking cyber risk to investment performance is information production: disclosures, reporting choices, and the surrounding regulatory environment shape how investors learn about latent vulnerabilities. Empirical work suggests that breach disclosures can increase subsequent stock price crash risk, indicating that cyber events may amplify downside asymmetry beyond short-lived announcement effects, especially when governance and information frictions are material (Cao et al., 2024). Regulation can further condition these outcomes by changing disclosure incentives and information quality. Disclosure

deadlines may accelerate reporting but reduce informational completeness, creating trade-offs that matter for how markets interpret delays, credibility, and uncertainty around remediation (Ashraf et al., 2022). Evidence also indicates that the disclosure vehicle itself can shape investor interpretation, with exploratory findings on cyber breach disclosures in 8-K filings suggesting that reporting form and timing can influence market responses and their persistence (Gordon et al., 2024).

Another cluster of studies highlights that cyber outcomes and market reactions are conditioned by governance and organizational capability rather than incident occurrence alone. Cyber risk management encompasses governance structures, control environments, incident response readiness, assurance arrangements, and investment prioritization that can vary widely across firms. Framework-oriented work argues that cybersecurity investment should be aligned with enterprise risk priorities and evaluated through explicit cost analysis, positioning cyber spending as a strategic capital allocation decision rather than a discretionary IT expense (Lee, 2021). Managerial human capital also appears relevant: executive IT expertise has been associated with differences in reported security breaches, suggesting that top management capabilities can shape prevention, detection, and incident governance quality (Haislip et al., 2021). Investor response can also be behavioral, as evidence shows cyber breaches can reduce investors' interest in a firm, implying that trust, perceived competence, and communication credibility may affect investment attractiveness alongside fundamentals (Demek & Kaplan, 2023).

Cyber risk can also extend beyond the breached firm through contracting and network spillovers that matter for investment conditions. Customer firm breaches

have been linked to higher audit fees for suppliers, implying that cyber events can raise monitoring costs and perceived risk across connected firms, with potential implications for financing costs and valuation (Zhang & Smith, 2023). Relatedly, breaches can surface through internal control consequences, reinforcing that cyber events may be interpreted as signals about governance and reporting reliability that investors track when forming performance expectations (Zhou & Huang, 2024). Taken together, the literature suggests that cyber risk management influences investment performance through a combination of priced exposure, disclosure-driven market learning, capability-based resilience, and spillover channels that reshape monitoring and trust.

3. Methods

The study adopts a systematic literature review design to synthesize peer-reviewed evidence on cyber risk management and investment performance. A structured search was conducted across major academic databases and indexing platforms, including Scopus and Web of Science, complemented by targeted retrieval through Google Scholar to capture relevant journal articles that may not appear uniformly across a single index. Search strings combined terms related to cybersecurity or cyber risk, risk management, breach disclosure, governance and controls, audit and assurance, and investment outcomes such as returns, valuation, risk premia, and crash risk. The review scope was limited to peer-reviewed journal articles published between 2019 and 2024 to maintain topical consistency and comparability of evidence.

Records were screened in stages to ensure relevance and quality. After duplicate removal, titles and abstracts were evaluated against predefined inclusion criteria, followed by full-text assessment to confirm that studies explicitly linked cyber risk or cyber risk management to investment-relevant outcomes. Eligible studies were coded using a standardized extraction template capturing context and sample, key constructs and proxies (including cyber risk management dimensions and investment performance measures), empirical approach, and principal findings. Evidence was synthesized thematically using a mechanism-based logic, organizing results around how cyber risk management may influence investment performance through priced exposure, disclosure and market learning, capability-based resilience, and spillover or contracting channels, while documenting boundary conditions and inconsistencies that inform research opportunities.

4. Results and Discussion

4.1. Cyber Risk and Investment Performance

Across the reviewed studies, the most consistent finding is that cyber risk becomes investment-relevant through two related pathways: realized incidents and underlying exposure. Realized incidents such as breaches can trigger direct and indirect cash-flow impacts (response costs, operational disruption, legal and regulatory penalties, and reputational damage), which often translate into negative valuation effects and revised expectations about future volatility. Underlying exposure matters even when no breach is observed, because investors can treat cyber vulnerability as a priced form of uncertainty that affects required returns and

portfolio positioning. Evidence that cybersecurity risk exposure is priced in the cross-section of stock returns supports the view that cyber risk is not merely idiosyncratic noise, but a factor that can influence investment performance via risk premia and investor demand for resilience (Florackis et al., 2023).

Importantly, "investment performance" is operationalized in more than one way in this literature, and that choice strongly shapes what is observed. Studies focusing on short event windows typically capture immediate repricing around breach-related news, while studies using broader proxies capture changes in expected returns, tail risk, and longer-horizon valuation effects. A robust pattern is that breaches can shift not only average returns but also the distribution of returns, particularly by increasing downside risk. For example, breach disclosures have been associated with higher subsequent stock price crash risk, consistent with heightened uncertainty and the possibility that cyber events reveal deeper governance and control weaknesses that investors previously underweighted (Cao et al., 2024). Taken together, the results imply that cyber risk affects investment performance through both level effects (valuation and returns) and risk effects (risk premia and tail risk), and synthesizing across these requires matching the outcome measure to the hypothesized channel.

4.2. How Cyber Risk Management Matters

The reviewed evidence suggests cyber risk management influences investment performance less by "eliminating" cyber threats and more by shaping four levers that markets price: loss severity, response reliability, information credibility, and external contracting costs. In this view, cyber risk management is a portfolio of

governance and investment decisions spanning control design, incident response readiness, and resource allocation discipline. Framework-oriented work argues cybersecurity investment should be evaluated through explicit cost analysis and integrated into enterprise risk priorities, positioning cyber spending as a capital allocation decision rather than a discretionary IT expense (Lee, 2021). Consistent with a capability-based interpretation, leadership and human capital also condition outcomes, as executive IT expertise has been associated with differences in reported data security breaches, implying that managerial competence can affect prevention, detection, and incident governance in ways investors may interpret as operational reliability (Haislip et al., 2021).

Assurance and monitoring further influence how credible those capabilities appear to external stakeholders. Evidence that cybersecurity audit effectiveness is associated with higher cyber risk management maturity supports the role of monitoring functions in institutionalizing controls and demonstrating preparedness, even when perfect prevention is unrealistic (Slapničar et al., 2022). This credibility component matters because cyber incidents are also information events: markets update beliefs about latent vulnerabilities based not only on what happened, but on whether the firm can show control quality and response discipline.

A substantial portion of the investment-performance effect therefore operates through market learning shaped by disclosure practices and regulatory constraints. Disclosure deadlines can speed reporting but reduce informational completeness, creating trade-offs that influence how investors interpret uncertainty, remediation credibility, and residual risk (Ashraf et al., 2022). Longitudinal evidence

also indicates that cybersecurity risk disclosures evolve in content and framing, reinforcing that disclosure is an ongoing channel through which investors reassess risk rather than a one-off reaction to a single event (Gao et al., 2020). Taken together, cyber risk management appears most investment-relevant when it both limits expected loss severity and communicates credibly enough to reduce information asymmetry and associated contracting frictions.

4.3 When Effects Differ and How They Are Measured

The review also shows that effects vary systematically across contexts and measurement choices, which explains why findings can appear inconsistent when compared naively. Several boundary conditions recur. Investor attention is one: breach announcements released when attention is distracted can generate muted immediate reactions, implying that event-study estimates may understate the true economic significance of cyber incidents and the value of risk management that prevents them (Foerderer & Schuetz, 2022). Governance and information frictions are another: the crash-risk evidence suggests cyber events are more damaging when they interact with opacity, weak oversight, or limited credibility, which can magnify downside asymmetry (Cao et al., 2024). Interdependence also matters: cyber risk can propagate via supply chains and contracting networks, shifting costs and risk assessments beyond the breached firm.

Measurement choices are central to interpreting these contingencies. Studies operationalize "cyber risk management" using proxies that range from disclosure language and governance attributes to audit effectiveness and managerial expertise, and these proxies do not all map to the same performance channel. Likewise,

"investment performance" can reflect short-run abnormal returns, longer-run expected returns, valuation ratios, crash risk, volatility, or contracting costs. The synthesis indicates that stronger alignment between construct and outcome improves interpretability: for example, governance and assurance proxies often align more clearly with tail-risk and credibility channels, while incident measures align more directly with event responses, and disclosure measures align with information asymmetry and market learning.

A recurring spillover insight reinforces why contracting channels should be part of investment-performance interpretation. Customer breaches have been associated with higher audit fees for suppliers, suggesting that cyber events can raise monitoring costs across connected firms and, by extension, influence financing conditions and valuation (Zhang & Smith, 2023). Complementing this, evidence links successful cyberattacks to firm value through mechanisms involving risk management and reputation, underscoring that trust and credibility can be economically consequential in capital markets (Kamiya et al., 2021). Overall, the combined evidence supports a mechanism-based conclusion: cyber risk management is most likely to translate into stronger investment performance when it is observable through credible governance and assurance, paired with disclosure practices that reduce ambiguity, and when performance is assessed using outcomes that capture risk and downside exposure rather than only short-window price reactions.

5. Conclusion

The reviewed evidence supports a consistent conclusion that cyber risk is financially material because it affects not only realized losses from incidents but also investor perceptions of latent exposure, downside tail risk, and resilience. Investment performance impacts therefore emerge through both level effects (valuation and returns) and risk effects (risk premia, volatility, and crash risk), with differences across studies often reflecting the specific performance proxies and time horizons used. In this sense, cyber risk management is best understood as an investment-relevant capability that can shape how markets price uncertainty and how firms sustain value under digital threat.

Across the literature, cyber risk management appears most consequential when it strengthens governance and investment discipline, improves response reliability, and enhances the credibility of control and assurance signals. Firms that embed cybersecurity within enterprise risk priorities, treat cyber spending as a capital allocation choice, and support it with effective monitoring are more likely to reduce expected loss severity and limit the persistence of negative market reappraisals. Disclosure practices further condition outcomes by influencing investor learning: when communication is timely, sufficiently informative, and aligned with regulatory expectations, it can reduce ambiguity and information asymmetry that would otherwise amplify downside penalties and contracting frictions.

Taken together, the synthesis suggests that future scholarship will benefit from tighter alignment between how cyber risk management is operationalized and which investment-performance channel is being tested, especially when claims

involve risk premia or tail risk rather than short-window announcement effects. More comparable measures of cyber capabilities and disclosure quality, combined with designs that explicitly test boundary conditions such as investor attention, industry digital intensity, and inter-firm dependence, would improve interpretability and causal inference. For practice, the evidence implies that treating cyber resilience as a strategic governance and investment issue, supported by credible assurance and disclosure, is more likely to translate into investment-relevant benefits than narrowly technical defenses alone.

References

Ashraf, M., Jiang, J. X., & Wang, I. Y. (2022). Are there trade-offs with mandating timely disclosure of cybersecurity incidents? Evidence from state-level data breach disclosure laws. *Journal of Finance and Data Science, 8*, 202-213.

Cao, H., Phan, H. V., & Silveri, S. (2024). Data breach disclosures and stock price crash risk: Evidence from data breach notification laws. *International Review of Financial Analysis, 93*, 103164.

Demek, K. C., & Kaplan, S. E. (2023). Cybersecurity breaches and investors' interest in the firm as an investment. *International Journal of Accounting Information Systems, 49*, 100616.

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies, 36*(1), 351-407.

Foerderer, J., & Schuetz, S. W. (2022). Data breach announcements and stock market reactions: A matter of timing? *Management Science, 68*(10), 7298-7322.

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems, 38*, 100468.

Gordon, L. A., Loeb, M. P., Zhou, L., & Wilford, A. L. (2024). Empirical evidence on disclosing cyber breaches in an 8-K report: Initial exploratory evidence. *Journal of Accounting and Public Policy, 46*, 107226.

Haislip, J., Lim, J.-H., & Pinsker, R. (2021). The impact of executives' IT expertise on reported data security breaches. *Information Systems Research, 32*(2), 318-334.

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*(3), 719-749.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons, 64*(5), 659-671.

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems, 44*, 100548.

Zhang, Y., & Smith, T. (2023). The impact of customer firm data breaches on the audit fees of their suppliers. *International Journal of Accounting Information Systems, 50*, 100628.

Zhou, F., & Huang, J. (2024). Cybersecurity data breaches and internal control. *International Review of Financial Analysis, 93*, 103174.