An Integrated Framework for Ransomware Mitigation: A NIST-Aligned Defense Model Linking Cyber Insurance and Risk Management

Li Huang and Kimberly A. Cornell
University at Albany, USA

lhuang9@albany.edu
kacornell@albany.edu

Abstract: Ransomware attacks have become one of the most disruptive cyber threats to modern organizations, causing significant financial losses, operational disruptions, and reputational damage across sectors. While organizations increasingly adopt security measures to mitigate risks, the fast-evolving role of cyber insurance-supported mitigation services in ransomware defense remains insufficiently understood. Cyber insurance has evolved from just a reactive compensator to a proactive security partner. It now offers pre-incident services to mitigate attack severity and post-incident services for quick recovery, reducing loss impacts. Cyber risk management and cyber insurance practices are often divided among different disciplines. Actuarial underwriting seldom integrates risk management models, and cybersecurity experts rarely include insurer mitigation tools in governance plans. This disjointed approach restricts organizations from effectively using insurance services as part of a comprehensive ransomware resilience strategy. This study investigates how cyber insurance-supported services aligned with the NIST Cybersecurity Framework reduce the impact of ransomware incidents. Building on prior empirical research identifying socio-technical drivers of ransomware losses, this paper proposes an integrated mitigation framework that combines security governance functions with insurance-supported services including vulnerability assessment, forensic readiness, incident response coordination, and recovery assistance. The framework conceptualizes ransomware risk mitigation as a layered process in which socio-technical risk drivers shape both the likelihood of incidents and the effectiveness of mitigation mechanisms. By incorporating the socio-technical factors that shape the impact of ransomware incidents, the proposed framework provides a more comprehensive defense posture against ransomware threats. Through analytical modeling and scenario-based evaluation, this study demonstrates how coordinated implementation of NIST-aligned cyber insurance services can significantly reduce expected ransomware losses and accelerate organizational recovery. The findings emphasize integrating technical cyber practices with insurance expertise to strengthen cyber resilience. By linking cyber risk management and insurance, this research enhances understanding of ransomware mitigation and offers practical insights for organizations managing ransomware risks in a rapidly evolving threat landscape.

Keywords: Ransomware Attacks, NIST CSF, Cyber Insurance Service, Integrated Framework, Risk Mitigation

1. Introduction

Ransomware attacks have become one of the fastest-growing cybercrimes in the digital economy (Sausalito, 2024). Organizations across industries increasingly rely on information systems to support critical operations, making them attractive targets for cyber adversaries. Cybercriminals use ransomware to encrypt victims' sensitive information and threaten to publicly release the information unless a ransom payment is made (August, et al., 2019; OZ, et al., 2022). Recent reports indicate that ransomware incidents continue to grow in frequency and severity, leading to billions of dollars in economic losses each year (Cartwright & Cartwright, 2023). Ransomware attacks can disrupt essential services, compromise sensitive data, and undermine trust in digital infrastructure (Dawson, et al., 2021). As tactics evolve toward professionalized models a variety of crimes like double and triple extortion, supply-chain propagation, and Ransomware-as-a-Service have emerged that traditional cybersecurity defenses alone are often insufficient to mitigate ransomware impact (Nagar, 2024).

To address this threat, many technology-based solutions have been developed to protect information assets (Hegde & Rokseth, 2020). As ransomware attackers target vulnerabilities in system and employee behavior, non-technical factors have become crucial in cyber defense (Nagar, 2024; Shaikh, et al., 2024). Various management frameworks address the growing complexity of cyber-attacks (Rassam, et al., 2017). These frameworks guide organizations in managing cyber risks, incident handling, and prevention. Organizations select frameworks or combinations that suit their needs to enhance cybersecurity and protect digital assets. The NIST Cybersecurity Framework (CSF) is widely used, categorizing practices into five domains: Identify, Protect, Detect, Respond, and Recover (NIST, 2022). These domains provide an approach to organizations for managing cyber risks across the entire lifecycle of a cyber incident (NIST, 2022).

Cyber insurance has been evolving beyond the traditional insurance paradigm to embrace security expertise (Huang & Cornell, 2025; Zywave, 2025). Risk services alongside cyber insurance policies help prevent potential

threats and mitigate the impacts of cyber incidents (Zeller & Scherer, 2023). Cyber insurance in recent years has increasingly evolved into a provider of cybersecurity expertise and mitigation services (Huang & Cornell, 2025; Zywave, 2025; Blackfog, 2024). Modern cyber insurance policies often include pre-incident and post-incident support such as vulnerability assessments, incident response coordination, digital forensics, and recovery assistance (Zeller & Scherer, 2023). These services position insurers as active participants in cybersecurity governance rather than passive claim processors (Huang & Cornell, 2025; Blackfog, 2024). As cyber threats continue to escalate, the role of cyber insurance is shifting toward a more proactive model that emphasizes prevention and resilience. This proactive capability may help position cyber insurance in a more central position in cyber risk management.

Despite advancements, a gap still exists in understanding how cyber insurance reduces ransomware risks. Existing literature mainly examines technologies, governance frameworks, or cyber insurance mechanisms independently (McIntosh, et al., 2021). Technical studies typically focus on detection algorithms, system hardening, or network defense mechanisms, while economic and actuarial research examines cyber insurance pricing and risk transfer (Martin & Collier, 2020). Ransomware mitigation is inherently socio-technical requiring coordination between technical defenses, organizational practices, and financial risk management mechanisms (Mukhopadhyay & Jain, 2024). The effectiveness of ransomware mitigation strategies may depend on socio-technical conditions within organizations. For example, organizations with stronger security governance may be able to leverage incident response services more effectively, while highly interconnected organizations may face greater challenges in containing ransomware propagation. Previous work does not fully capture how mitigation effectiveness emerges from the interaction between internal governance mechanisms and external risk management services under varying organizational conditions. This fragmentation limits the theoretical understanding and practical application of defenses.

This study examines how cyber insurance-supported services aligned with the CSF mitigate ransomware impacts. Incorporating socio-technical drivers of ransomware losses, the paper proposes an integrated analytical framework that links organizational risk drivers, cybersecurity governance functions, and insurance-supported mitigation services. Mitigation effectiveness is conceptualized as the outcome of coordinated security controls and insurance services operating across the ransomware attack lifecycle. The central theoretical contribution lies in demonstrating that mitigation effectiveness is not additive but interactional, where the marginal benefit of one mechanism depends on the presence of the other and is further conditioned by socio-technical factors such as organizational preparedness, technological posture, and network exposure. By formalizing these relationships, this study goes beyond descriptive integration and provides a structured explanation of how coordinated mitigation strategies produce non-linear reductions in ransomware impact. To our knowledge, this is among the first studies to formally model the interaction between cybersecurity governance and insurance-supported mitigation services in complex socio-technical environments.

The rest of this paper is organized as follows. Section 2 reviews related literature on ransomware risks, cybersecurity frameworks, and cyber insurance services. Section 3 presents the integrated mitigation framework and analytical model. Section 4 presents scenario-based analysis demonstrating the effectiveness of coordinated mitigation mechanisms. Section 5 discusses implications for cybersecurity governance and cyber insurance. Section 6 concludes with future research suggestions.

2. Literature Review

Ransomware has increasingly become a targeted attack, where attackers carefully select victims based on system vulnerabilities and data sensitivity (OZ, et al., 2022). As a result, socio-technical factors such as technical infrastructure, organizational readiness, and operational processes are vital in determining the impact of ransomware attacks (Haimes, 2012; Zhang, et al., 2011; Anderson & Moore, 2006). These factors not only influence the severity of ransomware incidents but may also affect the effectiveness of mitigation strategies. Addressing these factors is essential for accurate risk assessments and for proactive defense implementations. While previous studies highlight socio-technical factors in ransomware outcomes, many are descriptive and lack explicit links to mitigation effectiveness. They offer limited analysis of how organizational conditions affect mitigation mechanisms and loss severity, restricting practical risk management insights.

To address these complex cyber risks, organizations often rely on structured governance frameworks. Among the most widely adopted frameworks is the CSF, which provides a structured approach for identifying, assessing, and mitigating cybersecurity threats (NIST, 2022). Existing literature examines cybersecurity frameworks in strengthening organizational cyber resilience (Tsen, et al., 2022). However, these frameworks mainly emphasize technical and organizational controls within the firm. While providing valuable guidance for managing cyber risks,

they often do not explicitly incorporate external risk management mechanisms such as cyber insurance. Existing studies primarily emphasize internal governance structures and technical controls, treating organizations as self-contained units of defense. As a result, existing frameworks may overlook the wider ecosystem of actors involved in cyber risk mitigation.

Cyber insurance was initially a financial tool to compensate organizations for cyber losses (Blackfog, 2024). It has evolved to offer more cybersecurity services (Zywave, 2025; Huang & Cornell, 2025; Blackfog, 2024). Now cyber insurance provides pre- and post-incident risk assessment services, including vulnerability assessments, security audits, legal guidance, and response coordination (Zeller & Scherer, 2023). As incidents have increased in frequency and sophistication, cyber insurance has become more involved in helping organizations manage cybersecurity risks proactively (Mukhopadhyay & Jain, 2024). Cyber insurance increasingly functions as a risk advisor that supports organizations throughout the cybersecurity lifecycle. While industry reports highlight this service-oriented shift (Zywave, 2025), academic literature seldom explores how these services affect security controls or their impact on mitigation in various organizational contexts. This gap suggests the need for a more integrated analytical perspective that connects insurance-supported services with cybersecurity frameworks and socio-technical risk factors.

Although substantial research exists on ransomware, cybersecurity frameworks, and cyber insurance, these areas have largely developed independently. Technical ransomware research has focused primarily on detection algorithms, encryption mechanisms, and system defense strategies. Actuarial research on cyber insurance has concentrated on risk pricing and contract design. Few studies examine how insurance-supported mitigation services interact with governance frameworks under varying socio-technical conditions.

This study develops an integrated framework linking socio-technical ransomware risk drivers with NIST-aligned cyber insurance services. It aims to enhance understanding of ransomware mitigation strategies in modern cyber risk environments.

3. Conceptual Framework

While cybersecurity frameworks provide guidance for implementing technical and governance controls, cyber insurance offers additional resources and expertise that can support organizations in preventing, responding to, and recovering from cyber incidents. This study proposes an integrated mitigation framework that links cybersecurity governance functions with cyber insurance-enabled mitigation services to reduce ransomware impact. The proposed framework conceptualizes ransomware risk mitigation as a layered system consisting of three primary components: socio-technical risk drivers, cybersecurity governance mechanisms, and insurance-supported mitigation services. These components jointly determine the effectiveness of mitigation actions and ultimately influence ransomware outcomes.

3.1 Socio-Technical Drivers of Mitigation Effectiveness

Socio-technical conditions within organizations play an important role in determining the effectiveness of ransomware mitigation strategies (Mukhopadhyay & Jain, 2024). Cybersecurity systems operate within complex organizational environments where human behaviour, technological infrastructure, and organizational processes interact (Neoaz, 2024). Consequently, the same mitigation mechanisms may produce different outcomes depending on organizational conditions.

- Organizational preparedness refers to the extent to which an organization has established cybersecurity governance structures, security awareness programs, and incident response planning capabilities. Organizations with stronger preparedness are better positioned to implement cybersecurity controls and respond effectively when ransomware incidents occur (Haimes, 2012).
- Technology posture reflects the quality and robustness of an organization's technological infrastructure, including system architecture, patch management practices, and network security configurations. Weak technological infrastructure may create vulnerabilities that ransomware attackers can exploit, thereby increasing both the likelihood and severity of incidents (Zhang, et al., 2011).
- Settlement duration captures the time required to resolve ransomware incidents, including negotiation processes and system restoration efforts. Longer settlement durations often indicate more severe operational disruption and may increase overall financial losses (Anderson & Moore, 2006).

- Network exposure represents the extent to which organizations are connected to external partners, vendors, and digital supply chains. Highly interconnected systems may increase the potential for ransomware propagation across networks, making containment and recovery more difficult (Robinson, et al., 2022).

These socio-technical factors influence ransomware mitigation in two ways: they impact the likelihood and severity of ransomware incidents, and they shape the effectiveness of mitigation mechanisms implemented through cybersecurity frameworks and insurance-supported services.

3.2 Integration with CSF and Cyber Insurance Services

The framework integrates ransomware-relevant mitigation strategies across the five functions of the CSF, demonstrating how technical controls, governance practices, and cyber insurance services operate together throughout the ransomware lifecycle. Table 1 organizes the proposed framework along two dimensions: (1) the five functional domains of the CSF, and (2) three complementary layers of mitigation, cyber insurance-supported services, internal cybersecurity controls, and socio-technical influencing factors. Rather than representing independent components, the table illustrates how these elements operate jointly within each stage of the ransomware lifecycle. Specifically, each column represents a governance phase (from Identify to Recover), while each row highlights how different mitigation resources and contextual conditions contribute to reducing ransomware risk within that phase. This structure emphasizes that mitigation effectiveness emerges from the coordination of technical controls, external expertise, and organizational conditions rather than from any single mechanism in isolation.

Table 1: Integrated Framework

NIST	Identify	Protect	Detect	Respond	Recover
Cyber Assistance	IT Asset Inventory, Vulnerability Assessment	Employee upskilling, Awareness Training, Encryption & Backup	Monitor, Alert Suspicious Information Flows, Block Payload	Forensics, Quarantine Infected Systems, Intelligence Cooperation (e.g., Extortion Consulting)	Data Restoration, Business Continuity, Review & Fix
Empirical Measures	Supply Chain Risk Management, End-of-life Systems Protection, Logging and Monitoring Protections	MFA, Patch Management, Email Filtering, RDP, Awareness Training, Backup	EDR, Logging and Monitoring Protections, Early Detection of Threats	Ransomware Incident Response Plan, Negotiation, Legal Consulting	End-of-life Systems Protection, Backup, PAM
Influencing Factors	Technical Vulnerabilities, Organizational Preparedness	Technical Vulnerabilities, Organizational Preparedness	Organizational Preparedness	Breadth of Impacted Entities, Duration of Incident Resolution	Technical Vulnerabilities, Breadth of Impacted Entities

Table 1 represents a layered interaction model rather than a static mapping of controls. Within each NIST function, cyber insurance services complement internal cybersecurity capabilities by extending organizational resources, while socio-technical factors condition the effectiveness of both. As a result, mitigation mechanisms are context-dependent rather than universally effective. For example, vulnerability assessments in the Identify phase are more effective in organizations with higher preparedness, and incident response coordination in the Respond stage produces greater loss reduction when organizational processes enable rapid decision-making.

In summary, these integrated activities illustrate how NIST-aligned security functions and insurance-enabled services can operate as a unified defense structure rather than as separate or sequential mechanisms.

3.3 Analytical Representation of the Mitigation Framework

To formalize the relationships illustrated in the framework, ransomware impact is modeled as a function of socio-technical risk drivers and mitigation mechanisms. Let the expected ransomware loss for organization *i* be represented as:

$$Loss = f(RiskDriver\_i, Mitigation\_i)$$

where *RiskDrivers* represents organizational conditions such as preparedness, technological posture, settlement duration, and network exposure, and *Mitigation* represents the combined effect of cybersecurity governance controls and insurance-supported services.

Mitigation consists of cyber risk controls embedded the NIST framework and insurance-supported mitigation services. It is not treated as a single aggregated input but as a structured combination of interacting components:

$$Mitigation = g(NISTControls, InsuranceServices, RiskDrivers)$$

Where *NISTControls* denotes internal cybersecurity controls aligned with NIST functions, and *InsuranceServices* represents external mitigation services from cyber insurance. The inclusion of *RiskDrivers* within the mitigation function reflects the context-dependent nature of mitigation effectiveness, indicating that the same mitigation strategy may have different outcomes across organizational environments.

This formulation implies two key points. First, mitigation exhibits a complementary effect, where the marginal effectiveness of cybersecurity controls increases in the presence of insurance-supported services. Second, mitigation is conditional, which means socio-technical factors moderate the relationship between mitigation measures and ransomware outcomes. For instance, organizations with higher preparedness may benefit more from incident response services, while highly exposed networks may reduce the effectiveness of detection mechanisms.

Together, these relationships define a non-linear mitigation structure in which ransomware loss reduction depends on both the interaction between mitigation components and the organizational context in which they are deployed. This analytical representation provides a formal foundation for the simulation model developed in the upcoming section. This structure differs from previous models that assume additive mitigation effects by explicitly incorporating interaction terms between governance controls and insurance services.

4. Research Design

To evaluate the effectiveness of ransomware mitigation strategies, this study adopts a quantitative test based on scenario-based simulation. The purpose of this approach is to test conceptual modeling while addressing limitations in publicly available ransomware datasets. Public cyber incident datasets typically provide detailed information about attack vectors, affected sectors, and incident characteristics, but they rarely capture the full range of mitigation services associated with cyber insurance or coordinated incident response efforts. As a result, relying exclusively on observed data may not fully capture the interaction between cybersecurity governance mechanisms and insurance-supported mitigation services. To address this limitation, a Monte Carlo simulation is implemented to examine how different mitigation configurations influence ransomware outcomes across organizational environments. This approach enables the study to evaluate both the direct effects of mitigation mechanisms and the conditional effects shaped by socio-technical risk drivers, providing a structured empirical basis for assessing the integrated mitigation framework proposed in Section 3. The simulation is designed as a theory-consistent evaluation rather than a predictive empirical model.

4.1 Simulation Method

To ensure reproducibility, the key socio-technical variables are operationalized as follows. Organizational preparedness is modeled as a continuous variable in the range [0,1], representing the maturity of governance structures, incident response planning, and security awareness. Technology posture represents the robustness of technical infrastructure (e.g., patching, system hardening), which is normalized to [0,1]. Network exposure reflects the degree of external connectivity and third-party dependencies, between 0 and 1, where higher values indicate greater exposure to propagation risk. Settlement duration is a positive continuous variable representing the time required to resolve ransomware incidents. These variables are treated as stochastic inputs in the simulation and jointly determine both baseline risk and mitigation effectiveness.

Two categories of mitigation mechanisms are incorporated into the model.

- CSF functions which represent internal organizational cybersecurity capabilities.
- Insurance-supported mitigation services, such as vulnerability assessments, digital forensics support, incident response coordination, recovery assistance. These services represent external resources that complement internal cybersecurity capabilities.

We identify the dependent variable as Ransomware Impact.

Ransomware impact represents the severity of consequences experienced by an organization following a ransomware attack. Because financial loss data are often incomplete in public disclosures, a composite impact indicator can be constructed based on observable incident outcomes. The ransomware impact variable may include indicators such as operational disruption duration, extent of system compromise, data exfiltration occurrence, recovery complexity. In analytical terms, ransomware impact can be represented as a continuous severity measure or as a categorical indicator of high-impact incidents.

A Monte Carlo simulation is used to generate a synthetic population of organizations with varying socio-technical characteristics. In the simulation, socio-technical variables are generated from bounded probability distributions to reflect heterogeneous organizational environments. Specifically, preparedness and technology posture are drawn from Beta distributions to capture variability across organizations, while network exposure is modeled using a right-skewed distribution to reflect the prevalence of highly connected systems. Settlement duration is generated from a log-normal distribution to capture the heavy-tailed nature of incident resolution time. The simulation is conducted over 10000 iterations to ensure stability of the results. Parameter values are selected to reflect realistic ranges observed in previous cyber risk studies, while allowing sufficient variability to examine relative mitigation effects across different organizational contexts.

Consistent with Section 3's framework, ransomware impact is computed as a function of baseline risk adjusted by mitigation effectiveness. Mitigation effects are modeled as multiplicative reductions in expected loss, allowing for interaction between cybersecurity controls and insurance-supported services. This structure captures both independent and joint effects of mitigation mechanisms and enables evaluation of complementarity across scenarios.

4.2 Result Analysis

We use Monte Carlo simulation to generate numerical values for the variables that are hard to observe. The synthesized data is used to evaluate how mitigation mechanisms influence ransomware impact. We show an example of model-generated results indicating the effectiveness of mitigation measures across four socio-technical contexts. While the results are not from real-world estimates, they provide a theory-consistent illustration of relative mitigation effects under uncertainty and support the study's modeling contribution. We present a flexible framework that adapts as more ransomware incident data emerges, assisting future researchers in analyzing evolving ransomware risks and mitigation strategies.

Table 2: Simulation Results

	Overall Sample (Baseline)		Weak Organizations (low preparedness / weak technology / high exposure)		Strong Organizations (high preparedness / stronger technology / lower exposure)	
Scenario	**Expected Loss**	**Reduction vs. No Mitigation**	**Expected Loss**	**Reduction vs. No Mitigation**	**Expected Loss**	**Reduction vs. No Mitigation**
No Mitigation	411097	-	943115	-	97814	-
CSF	262423	36.2%	648933	31.2%	48374	50.5%
Insurance Service	282434	31.3%	675968	28.3%	58661	40.0%
Integrated	163269	60.3%	429098	54.5%	23768	75.7%

Table 2 shows mean expected losses over 10000 simulations and relative reductions versus baseline. These values, consistent with the model's expectations, highlight differences in mitigation effectiveness rather than precise estimates. The results reveal several important insights regarding the effectiveness of ransomware mitigation strategies across different organizational contexts. First, mitigation effectiveness is context-dependent rather than universal. The same mitigation strategies produce different outcomes depending on

organizational preparedness and technological capability. For example, organizations with weaker preparedness experience substantially higher baseline expected losses compared with stronger organizations, indicating that organizational conditions significantly influence ransomware risk exposure.

Second, integrated mitigation strategies outperform isolated approaches. While both the CSF–based controls and cyber insurance individually reduce expected losses, their combined implementation produces the largest reduction across all scenarios. In the overall sample, the integrated strategy reduces expected losses by approximately 60.3%, compared with 36.2% for NIST-only mitigation and 31.3% for insurance-only mitigation. This finding suggests that technical controls and financial risk transfer mechanisms function most effectively when implemented together.

Third, organizational strength enhances mitigation effectiveness. Under the integrated scenario, ransomware loss reductions are about 54.5% for weak and 75.7% for strong organizations, showing that stronger security and lower exposure improve mitigation investments effectively. This result supports the study's socio-technical perspective that mitigation outcomes depend on both mechanisms and the organizational environment.

To summarize, these results highlight the importance of embedding cyber insurance-supported measures into institutional mechanisms such as CSF to achieve more robust ransomware risk mitigation.

5. Implications

This study's findings have important implications for both ransomware risk management and cyber insurance practice. The simulation results indicate that ransomware mitigation is most effective when internal cybersecurity controls and insurance-supported services are implemented as complementary rather than independent mechanisms. The integrated mitigation scenario consistently produced the greatest reduction in expected ransomware losses across all organizational contexts, outperforming both NIST-only and insurance-only approaches. This suggests that ransomware resilience should be understood not as the product of a single control domain, but as the outcome of coordinated socio-technical and institutional defenses.

From a governance perspective, the results emphasize CSF's value as a structured foundation for ransomware preparedness, detection, response, and recovery. However, the findings also suggest that internal governance mechanisms alone may be insufficient, particularly for organizations with weak preparedness, limited technological maturity, and high exposure. In such contexts, external support provided through cyber insurance services can extend organizational capabilities by supplying specialized expertise in vulnerability assessment, incident response coordination, forensic investigation, legal support, and recovery planning. Accordingly, organizations should move beyond viewing cyber insurance solely as a financial backstop and instead treat it as an operational component of cyber resilience strategy. This interpretation supports the proposed framework in this study, which positions insurance-supported services embedded in NIST-aligned functions across the ransomware lifecycle.

For cyber insurance, the findings support its latest trends: shifting from risk mitigator to proactive monitor and advisor, as it merges with cybersecurity services. In the model, insurance cyber services contributed to reduced expected ransomware impact by improving response capacity, accelerating recovery, and reducing the operational severity of incidents. This implies that cyber insurance can add strategic value through service design, vendor coordination, incident preparedness, and pre- and post-incident resilience assistance. Insurers may benefit from structuring policies to more explicitly align risk assessment and service provision with recognized governance frameworks such as the CSF. Through this alignment, cyber insurance can contribute to reducing organizational losses by encouraging proactive risk prevention, strengthening organizations' cybersecurity capabilities, and mitigating the severity of cyber incidents.

This study contributes to the growing recognition that ransomware is a socio-technical risk requiring interdisciplinary solutions. The simulation results show that mitigation outcomes depend not only on the presence of technical controls but also on preparedness, infrastructure quality, exposure, and recovery conditions. This has policy relevance as regulators, industry groups, and cybersecurity standards bodies may wish to promote better coordination between organizational security governance and cyber insurance ecosystems. Such coordination could support more consistent expectations regarding minimum controls, incident reporting, vendor engagement, and recovery planning, particularly in sectors facing systemic ransomware risk.

Overall, the central implication of this study is that effective ransomware mitigation requires integration. Organizations, insurers, and cybersecurity experts should move beyond fragmented approaches and instead

adopt coordinated defense models that combine governance frameworks, operational capabilities, and insurance-supported services into a unified strategy for cyber resilience.

6. Conclusion

Ransomware is a major cyber threat causing operational and financial damage. While organizations use cybersecurity frameworks and cyber insurance separately, they often lack a coordinated resilience approach. This study proposes an integrated framework combining cybersecurity practices with NIST-aligned insurance services to mitigate ransomware across various organizations.

Using Monte Carlo simulation, the study examined how different mitigation strategies influence expected ransomware losses under various socio-technical conditions. The results reveal three key findings. First, mitigation effectiveness depends on context, with organizational preparedness, technological capability, and exposure levels significantly affecting losses. Second, integrated mitigation strategies outperform isolated approaches. While NIST-based controls and cyber insurance each reduce losses, their combined implementation produces the largest impact. Third, organizations with stronger preparedness and tech capabilities benefit more from mitigation efforts, underscoring the importance of organizational readiness.

The primary contribution of this study is methodological. The paper introduces a modeling framework that integrates socio-technical risk conditions, governance controls, and insurance-supported mitigation services into a unified analytical structure. By linking cybersecurity governance with cyber insurance services, the framework provides a systematic approach for analyzing how different mitigation strategies interact to influence ransomware outcomes. This approach contributes to the interdisciplinary research that views ransomware not only as a technical threat but also as a risk management challenge.

There are some limitations. The simulation results rely on synthesized data designed to illustrate relative mitigation effects rather than precise real-world loss estimates. As a result, the findings should be interpreted as analytical demonstrations rather than empirical predictions. Despite these limitations, the study provides a structured foundation for understanding how integrated mitigation strategies can improve ransomware resilience. The framework proposed in this study offers a step toward developing more comprehensive and adaptive strategies for managing ransomware risk in complex socio-technical environments.

Future research can extend this work by incorporating real ransomware incident datasets, sector-specific risk parameters, and longitudinal analysis of mitigation effectiveness. These directions would empirically test the proposed framework and further validated in practical cybersecurity environments.

Ethical Declaration: Ethical approval was not required.

AI Declaration: AI tools were not used in the creation of this paper.

References

Anderson, R. & Moore, T., 2006. The Economics of Information Security. *Science,* 314(5799), pp. 610-613.

August, T., Dao, D. & Niculescu, M. F., 2019. *Economics of Ransomware.* s.l.:SSRN.

Blackfog, 2024. *Ransomware: The role of cyber insurance in protecting businesses.* [Online] Available at: https://www.blackfog.com/ransomware-cyber-insurance/ [Accessed 3 11 2025].

Cartwright, A. & Cartwright, E., 2023. The Economics of Ransomware Attacks on Integrated Supply Chain Networks. *Digital Threats 4,* 56(14), pp. 1-56.

Dawson, M., Bacius, R., Gouveia, L. & Vassilakos, A., 2021. Understanding the Challenge of Cybersecurity in Critical Infrastructure Sectors. *Land Forces Academy Review,* 26(1), pp. 69-75.

Denning, D., 2000. Reflections on Cyberweapons Control. *Computer Security Journal,* Issue 4, pp. 43-53.

Haimes, Y., 2012. Strategic Preparedness for Recovery from Catastrophic Risks to Communities and Infrastructure Systems of Systems. *Risk Analysis: An International Journal,* 32(11), pp. 1834-1845.

Hegde, J. & Rokseth, B., 2020. Applications of Machine Learning Methods for Engineering Risk Assessment - A Review. *Safety Science,* p. 104492.

Huang, L. & Cornell, K. A., 2025. *From Payer to Protector: the Evolving Role of Cyber Insurance in Ransomware Defense.* Charlottesville, IEEE Xplore.

Martin, A. & Collier, J., 2020. Beyond awareness: Reflections on Meeting the Interdisciplinary Cyber Skills Demand. *Cyber Security Education,* pp. 55-73.

McIntosh, T. et al., 2021. Ransomware Mitigation in The Modern Era: A Comprehensive Review, Research Challenges, and Future Directions.. *ACM Computing Surveys (CSUR),* 54(9), pp. 1-36.

Mukhopadhyay, A. & Jain, S., 2024. A Framework for Cyber-risk Insurance Against Ransomware: A Mixed-method Approach. *International Journal of Information Management,* Volume 74, p. 102724.

Nagar, G., 2024. The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies. *Valley International Journal Digital Library,* pp. 1282-1298.

Neoaz, N., 2024. Cybersecurity and Information Assurance: Bridging the Gap. *International Journal of Social, Humanities and Life Sciences,* 2(1), pp. 37-46.

NIST, 2022. *Cyber Attack.* [Online] Available at: https://csrc.nist.gov/glossary/term/cyber_attack [Accessed 22 8 2025].

OZ, H. O., Aris, A., Levi, A. & Uluagac, A., 2022. A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. *ACM Computing Surveys (CSUR),* 54(11), pp. 1-37.

Rassam, M., Maarof, M. & Zainal, A., 2017. Big Data Analytics Adoption for Cybersecurity: A Review of Current Solutions, Requirements, Challenges and Trends. *Journal of Information Assurance & Security,* 12(4).

Robinson, A., Corcoran, C. & Waldo, J., 2022. *New Risks in Ransomware: Supply Chain Attacks and Cryptocurrency,* s.l.: s.n.

Sausalito, C., 2024. *Why ransomware attacks are on the rise.* [Online] Available at: https://www.nationwide.com/business/solutions-center/cybersecurity/rise-in-ransomware-attacks [Accessed 11 12 2024].

Shaikh, M. U. R. et al., 2024. Fortifying Against Ransomware: Navigating Cybersecurity Risk Management with a Focus on Ransomware Insurance Strategies. *International Journal of Academic Research in Business & Social Sciences,* 14(1), pp. 1415-1430.

Tsen, E., Ko, R. & Slapnicar, S., 2022. An Exploratory Study of Organizational Cyber Resilience, Its Precursors and Outcomes. *Journal of Organizational Computing and Electronic Commerce,* 32(2), pp. 153-174.

Zeller, G. & Scherer, M., 2023. Risk Mitigation Services in Cyber Insurance: Optimal Contract Design and Price Structure. *Issues and Practice,* Issue 2, p. 502.

Zhang, Y. Z. et al., 2011. Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids. *IEEE Transactions on Smart Grid,* Issue 4, pp. 796-808.

Zywave, 2025. *Navigating the Escalating Risk Trajectory.* [Online] Available at: https://www.zywave.com/blog/2025-risk-report/ [Accessed 1 7 2025].