Quantifying the Economic Impact of Ransomware: Cyber Risk Modeling with Gamma Regression

Li Huang and Kimberly Cornell
University at Albany, USA

lhuang9@albany.edu
kacornell@albany.edu

Abstract: Ransomware has evolved into one of the most disruptive forms of cybercrime, resulting in severe financial and operational losses for organizations across various sectors. Despite its increasing prevalence, quantitative models for evaluating the drivers of ransomware losses remain underdeveloped, limiting both academic insight and practical risk management. This study addresses this gap by developing and empirically validating a statistical framework for quantifying the financial impact of ransomware incidents. Drawing on ransomware cases extracted from the Advisen Cyber Loss Database, we employ a generalized linear model (GLM) with Gamma regression and log link to estimate how socio-technical factors shape loss severity. Our analysis examines four categories of predictors: (1) Technology, operationalized via database server involvement in incidents; (2) Preparedness, captured through insurance coverage ratios; (3) Settlement Length, reflecting negotiation and resolution timelines; and (4) Multi-entity Connections, representing the number of affected organizations in an incident. The results indicate that each factor influences the anticipated magnitude of losses. Insufficient preparedness is correlated with greater financial damages, whereas incidents involving database servers and prolonged settlement periods result in disproportionately substantial losses. Moreover, multi-entity connections exacerbate losses due to cascading effects across organizational networks. To assess the robustness of the model, bootstrapping techniques are employed, confirming the stability of the coefficient estimates and underscoring the model's reliability under resampling. By providing empirical evidence of the drivers of ransomware loss severity, this study contributes to both academic research and practical cybersecurity governance. For scholars, it demonstrates the utility of Gamma regression in modeling highly skewed cyber loss distributions. For practitioners, it highlights quantifiable indicators that can inform cybersecurity investment and organizational preparedness strategies. More broadly, the findings highlight the importance of interdisciplinary approaches that integrate cybersecurity management with socio-technical dimensions of cyber risk. This work lays a foundation for future studies that extend to newer datasets and explore AI-enhanced risk prediction, thereby advancing both theoretical understanding and applied resilience against ransomware in the evolving cyber threat landscape.

Keywords: Ransomware attacks, Cyber risk management, Quantitative modelling, Organizational resilience

1. Introduction

Ransomware has become a targeted attack, primarily aimed at maximizing monetary gains (August, et al., 2019). However, modern ransomware operations have shifted toward a targeted attack, where attackers carefully select victims based on system vulnerability, data sensitivity, and willingness to pay a ransom (OZ, et al., 2022). This shift is driven by profit-maximization, as attackers seek to extract the highest possible payouts (Samonas, et al., 2020). Since ransomware attacks are deliberately targeted rather than purely opportunistic, organizations must assess their specific risk profiles rather than relying solely on generic malware defenses. In evaluating ransomware risks, non-technical factors, such as industry characteristics, cybersecurity preparedness, and overall vulnerability, play a crucial role in determining the impact of ransomware attacks. Understanding these factors enables more accurate risk assessments and the implementation of proactive defense.

Non-technical factors, such as industry sector, shape how an organization responds to an attack and influence the overall expected losses. For instance, organizations in critical sectors (e.g., healthcare, finance, and law enforcement) prioritize operational continuity and the security of sensitive information (Dawson, et al., 2021; Tsen, et al., 2022). By incorporating these sociotechnical factors, cybersecurity researchers can better assess the full impact of ransomware incidents and implement more effective mitigation measures (Samonas, et al., 2020). Yet, to validate the influence of these factors, reliable empirical data is essential.

However, one persistent challenge in ransomware research is the limited availability of high-quality empirical data. Many studies rely on simulated data, limited case studies, or proprietary industry reports that lack transparency or reproducibility (Anderson, et al., 2013). Due to privacy concerns and reputational risks, organizations underreport ransomware incidents, which results in under-sampled and biased datasets (Dekker & Karsberg, n.d.; Rassam, et al., 2017). Without comprehensive empirical data, it is difficult to validate theoretical models or accurately quantify economic impact. As a result, despite growing scholarly and industrial attention, limited research has quantitatively examined how socio-technical factors determine the financial impact of ransomware attacks. Prior studies have mainly focused on technical detection and response

mechanisms, leaving a gap in data-driven understanding of the economic consequences and risk drivers of ransomware.

To address this gap, we develop a quantitative framework that combines insights from cyber risk management and actuarial modeling. Drawing on the Advisen Cyber Loss Database (Advisen Insurance Intelligence, 2015) that integrates comprehensive data on cyber incidents resulting in substantial monetary losses, we empirically estimate ransomware loss severity using a Gamma regression model validated through bootstrapping. This approach advances current discourse by providing statistically grounded evidence on the drivers of ransomware losses and by identifying measurable indicators that can inform both academic research and practical cybersecurity management. Our focus encompasses the following: initially, we analyze the factors that influence the impact of ransomware risks, particularly those analogous to the determinants used in estimating the impact of data breaches. These factors include organizational structures, technological components, and vulnerabilities. Subsequently, we assess the monetary implications associated with ransomware attacks. According to McIntosh et al., ransomware losses are affected by attack duration, vulnerabilities, technological aspects, and connectivity (McIntosh, et al., 2021).

The remainder of this paper is organized as follows. Section 2 reviews the existing literature on ransomware and socio-technical determinants of cyber risk. Section 3 outlines the quantitative research framework, data description, and variable construction. Section 4 presents the empirical model, estimation procedures, and validation strategy. Section 5 analyzes the results and discusses implications for cybersecurity management. Finally, Section 6 concludes with key findings, limitations, and directions for future research.

2. Literature Review

Ransomware has evolved from opportunistic attacks to sophisticated, profit-driven operations that exploit both technical vulnerabilities and organizational weaknesses (August, et al., 2019; OZ, et al., 2022). This shift has intensified the financial burden on organizations and has drawn increasing scholarly attention. However, existing ransomware studies remain fragmented across multiple disciplines, including computer science, information systems, economics, and organizational studies. This disciplinary fragmentation often leads to isolated approaches to understanding and addressing the fast-evolving cyber threat (Martin & Collier, 2020; Neoaz, 2024). Most prior studies examine technical detection or incident response rather than the socioeconomic determinants of ransomware impact (Samonas, et al., 2020; Mukhopadhyay & Jain, 2024). Yet a comprehensive knowledge of ransomware requires an integrated perspective that considers technology, organizational behavior, and economic incentives. Despite a recognized need for interdisciplinary approaches, few studies have attempted to integrate socio-technical dimensions while quantifying ransomware risks (Mukhopadhyay & Jain, 2024).

In addition, quantitative analysis of ransomware loss severity remains limited. Although conceptual frameworks exist for valuing cyber risk, empirical validation with incident-level data is scarce (Anderson, et al., 2013). Moreover, recent research emphasizes that ransomware losses follow heavy-tailed, highly skewed distributions, requiring statistical methods beyond classical ordinary-least-squares assumptions (Mukhopadhyay, et al., 2019; Dutta & Perry, 2007; Edwards, et al., 2016). Gamma model best fits for positive, highly skewed data and is widely used in real-world applications including cyber-loss modelling (Ben-Assuli & Padman, 2020). However, few studies employ Gamma regression to capture cyber loss patterns. Addressing this methodological gap, we integrate socio-technical variables into a Gamma-based framework to estimate how the influencing factors discussed in the existing literature determine the impact of ransomware incidents.

Prior work identifies several socio-technical determinants of ransomware impact, summarized in Table 1.

Table 1: Synthesis for Socio-technical Determinants

Socio-technical Factor	Relevant Literature
Technology	First, the extent of technology usage in operational and business services significantly influences ransomware risks. For example, studies indicate that an increase in digital records correlates with a higher risk of ransomware attacks (Kim & Kwon, 2019). However, the impact of such attacks varies based on the specific IT components compromised. For instance, encrypting an internal system may result in lower losses compared to a server breach, as servers often contain more sensitive and critical information (Hoferek & Wilson, 2007). Furthermore, the number of digital assets influences potential ransomware risks. The more devices, applications, servers, and network components a company has, the greater the attack surface, and potentially more vulnerabilities to ransomware threats.

Socio-technical Factor	Relevant Literature
Vulnerability	An organization's IT environment plays a crucial role in assessing ransomware risks. No organization's cybersecurity is entirely immune to vulnerabilities that attackers can exploit (Gordon & Loeb, 2003). These vulnerabilities may exist in hardware, software, external connections, employee behavior, etc. Frameworks such as those provided by NIST offer guidance to enhance an organization's defenses against ransomware threats. The level of preparedness is directly related to the extent of these vulnerabilities (Haimes, 2012; Harkins & Freed, 2017). The better prepared an organization is, the fewer exploitable vulnerabilities it will have.
Settlement Length	When an organization's information assets are compromised, the financial losses are significantly influenced by the time taken to restore operations or negotiate with attackers. Extended downtime disrupts services and diminishes revenue (Brown, et al., 2019). Moreover, prolonged recovery time would damage reputation, as customers may lose confidence in the organization's ability to safeguard their data or maintain reliable service (Anderson & Moore, 2006).
Connection	Organizations operate within complex networks of suppliers, partners, and customers, and a ransomware attack can disrupt this entire ecosystem (Robinson, et al., 2022; Cartwright & Cartwright, 2023). The ripple effects of external connections often extend the impact beyond the organization itself (Okafor, et al., 2022). For instance, a logistics company hit by ransomware might cause delays across a supply chain, leading to financial losses for all affected stakeholders. Cybersecurity is a process, not a product. Cyber risk management should permeate every part of business operations.
Total Cost	Direct losses, such as ransom payments, are immediate and quantifiable financial losses. Expenditure spending to regain access to their encrypted data, such as hiring experts to patch vulnerabilities, also add to the financial burden. Organizations that handle sensitive or regulated data may face fines for failing to secure the information safety (Robinson, et al., 2022; Nagar, 2024).

However, these factors are often examined in isolation, without integrated empirical modeling that quantifies their combined influence on financial loss outcomes.

To address these gaps, this study applies a GLM with a Gamma distribution and log link, supported by bootstrapping validation. By integrating socio-technical factors, the proposed model empirically quantifies ransomware loss severity using real-world data from the Advisen Cyber Loss Database (2018–2020). This approach bridges technical and managerial research streams, offering both academic insight and practical indicators for cyber risk management.

3. Quantitative Research

This study adopts an interdisciplinary framework to quantify ransomware losses by integrating socio-technical factors of cyber risk. Drawing from the Advisen Cyber Loss Database, we identify ransomware incidents from 2018 to 2020 and examine their financial outcomes. The selection of the Advisen dataset is based on its well-established reliability and its comprehensive incident-level financial records. Compared to other proprietary or survey-based sources, Advisen provides more comprehensive coverage across sectors and includes verified financial outcomes, which makes it particularly suitable for quantitative modeling of ransomware impacts.

We operationalize four categories of predictors: technology, preparedness, settlement length, and multi-entity connections. These variables are chosen based on prior literature and their theoretical relevance to organizational resilience.

The methodological goal is twofold. First, to determine how socio-technical factors shape ransomware loss severity. Second, to establish an empirical model that is generalizable and robust enough to inform cyber risk management practices.

3.1 Hypothesis Development

Based on literature review and industry evidence, we formulate four hypotheses regarding determinants of ransomware losses:

> *Hypothesis 1 (H1): Incidents involving servers generate higher loss severity compared to non-server incidents.*

Database server involvement is treated as a binary variable (1 = server affected, 0 = otherwise). Prior studies show that server-related incidents compromise critical infrastructure and data availability, amplifying costs.

> *Hypothesis 2 (H2): Lower preparedness is associated with higher ransomware loss severity.*

Preparedness is measured through insurance coverage ratios, representing the proportion of losses covered by cyber insurance. Organizations with low preparedness (uninsured or underinsured) are hypothesized to experience higher effective losses.

Hypothesis 3 (H3): Longer settlement duration is positively associated with greater ransomware loss severity.

Length refers to the duration (days) between incident onset and settlement. Prolonged negotiations, technical issues, or legal disputes can cause operational disruptions and reputational damage.

Hypothesis 4 (H4): Incidents involving multiple entities are associated with disproportionately higher losses.

This variable represents the number of affected entities in each incident (e.g., supply chain or partner firms). Interconnected organizations amplify cascading risks.

These hypotheses collectively reflect the socio-technical nature of ransomware attacks, acknowledging that financial impact arises not only from technical vulnerabilities but also from organizational and relational contexts.

3.2 Data Description

The dataset is derived from the Advisen Cyber Loss Database, a widely used comprehensive dataset. We filter cases from 2018–2020 that are explicitly classified as ransomware events. This temporal window is chosen for two reasons: (1) ransomware attacks increased substantially and evolved in sophistication during this period, and more complete reporting became available; (2) the version of the Advisen dataset used in this study does not include ransomware incidents beyond 2020. This limitation is further discussed in a later section. However, the primary contribution of this study is its methodological framework, which remains applicable and adaptable as more recent ransomware incident data become available.

- Dependent Variable:

Loss Severity (continuous): the reported financial impact of the ransomware incident. Because of right-skewed distribution, it is modeled using Gamma regression.

- Independent Variables:

Preparedness (ratio, 0–1): extent of cyber insurance coverage.

Server Binary (dummy, 0/1): whether servers were directly affected.

Settlement Length (days): duration of ransomware attacks.

Affected Entities (count): number of organizations impacted.

A summary of variable descriptions and coding is provided in Table 2.

Table 2: Description of Variables

Variable	Denoted	Type	Definition	Classification
Total Financial Loss	TOTAL	DV	The financial damage due to ransomware incident	Continuous
Database Server	SERVER	IV	Whether database servers were directly affected	Binary
Preparedness	PREPARED	IV	The level of support from cyber insurance	Continuous
Settlement Length	LENGTH	IV	The duration of ransomware attacks	Discrete
Affected Entities	AFFECTED	IV	The number of organizations impacted	Continuous

3.3 Model Specification

Ransomware loss data is highly skewed, with many moderate losses and a small number of extreme cases. To capture this distribution, we employ a GLM with Gamma regression and log link. This choice is appropriate

because: (1) the Gamma family is well-suited for continuous, positive-valued outcomes with right-skew (Ben-Assuli & Padman, 2020; Edwards, et al., 2016); (2) the log link ensures multiplicative interpretation, meaning predictors indicate proportional changes in expected losses (Ben-Assuli & Padman, 2020). Thus, Gamma regression with log link provides a statistically robust approach for modeling the ransomware loss. The model is expressed as:

$$\ln(E[\text{TOTAL\_LOSS}_i]) = \beta_0 + \beta_1 \cdot \text{Preparedness}_i + \beta_2 \cdot \text{Server}_i + \beta_3 \cdot \text{Length}_i + \beta_4 \cdot \text{Affected}_i + \epsilon_i$$

To prepare the dataset, we retain outliers (extreme loss values beyond the 99th percentile) to preserve the distribution's integrity, while missing predictor values were imputed using median or mode as appropriate.

3.4 Validation Strategy

Given a limited sample size and skewed distributions, bootstrapping was used to evaluate the robustness of parameter estimates. Specifically, we conducted 100 resamples with replacement and recalculated coefficient estimates to generate empirical confidence intervals. This approach reduces reliance on asymptotic assumptions and ensures stability of findings under resampling variation.

All statistical analyses were conducted using R, a programming language designed for statistical analysis. Key packages include GLM for model fitting and boot for resampling. Data cleaning was performed using dplyr.

3.5 Summary

This methodology combines socio-technical insights with actuarial modeling to quantify ransomware loss severity. By focusing on four predictors—preparedness, server involvement, settlement length, and multi-entity connections—we establish an empirical framework that is both explanatory and predictive. The Gamma regression model with bootstrapping validation offers a statistically rigorous approach to understanding ransomware risks and provides practical indicators for insurers and policymakers.

4. Result Analysis

The regression results in Table 3 reveal several important insights regarding the factors influencing total reported losses from ransomware incidents.

Table 3: Gamma Regression Results (Log Link)

Variable	Estimate	Std. Error	z-value	p-value
Intercept	12.986	0.536	24.24	<0.001
PREPARED	11.002	11.133	0.99	0.323
AFFECTED	4.53e-11	7.09e-10	0.06	0.949
LENGTH	-0.0024	0.0006	-3.83	<0.001
SERVER	-53.018	0.536	-98.92	<0.001

Note: Dependent variable is TOTAL (total financial loss). Model uses a Gamma distribution with a log link. Significant predictors at $p < 0.05$ are in bold.

The intercept (estimate = 12.986, $p < 0.001$) represents the expected log-loss when all predictors are at their baseline levels, suggesting that even under minimal exposure conditions, ransomware incidents impose substantial financial burdens. The preparedness variable (PREPARED) shows a positive but statistically insignificant relationship with total loss, implying that the degree of insurance coverage does not consistently mitigate or amplify loss severity. This finding may reflect heterogeneity in policy structures, coverage limits, and reporting practices. Similarly, the coefficient for affected entities (AFFECTED) is near zero, indicating that the number of organizations linked to an incident does not meaningfully predict aggregate losses once other factors are controlled.

By contrast, the settlement length variable (LENGTH) has a significant negative relationship with total reported losses, which means prolonged negotiations may modestly reduce final loss amounts, possibly reflecting enhanced mitigation or recovery actions over time. The most notable effect emerges from database server involvement (SERVER). The large magnitude and statistical significance of this coefficient indicate that ransomware incidents involving database servers are associated with lower total reported losses, holding other factors constant. In other words, when ransomware attacks target database servers, organizations may experience comparatively reduced financial impacts relative to non-server incidents. This counterintuitive

finding may reflect underlying realities such as faster containment responses or earlier detection in server-related incidents. Regardless of the underlying causes, the result itself highlights the pivotal role of database server protection a mitigating potential financial losses from ransomware attacks.

4.1 Bootstrapping Validation

To assess the robustness of these results, Table 4 presents bootstrapping estimates derived from 100 resamples. The consistency of the coefficients across resampling reinforces the reliability of the model.

Table 4: Bootstrap Estimates for Gamma Regression Coefficients (100 Resamples)

Variable	Mean	Std. Dev.	2.5% CI	Median	97.5% CI
Intercept	12.412	1.005	10.656	12.893	13.858
PREPARED	14.093	20.514	-4.094	12.931	77.348
AFFECTED	3.08e-09	2.66e-08	-8.47e-09	1.47e-12	8.76e-09
LENGTH	0.0147	0.0306	-0.0066	-0.0019	0.0912
SERVER	-52.535	0.876	-53.858	-52.919	-50.967

The intercept remains stable (mean = 12.412, 95 % CI = 10.656–13.858), confirming a consistent baseline of ransomware loss magnitude. However, the preparedness variable (PREPARED) exhibits a large standard deviation (20.514) and an extremely wide confidence interval (–4.094 to 77.348), indicating instability and variability across resamples. This further supports the earlier conclusion that preparedness exerts no uniform or predictable influence on ransomware loss severity. Second, the affected entities variable (AFFECTED) retains an almost zero mean with a narrow confidence band centered around zero, reaffirming its negligible role in determining loss outcomes.

The bootstrap results confirm that the negative effects of both database server involvement (SERVER) and settlement length (LENGTH) are not only statistically significant in the original model but also consistently reproduced across resampled datasets. This consistency reinforces confidence in their robustness as key factors influencing total ransomware-related losses. LENGTH exhibits a generally negative trend, though with slightly greater variability, indicating a moderately consistent effect. SERVER shows strongly negative with a narrow confidence interval, reinforcing its role as a stable and influential predictor associated with lower reported losses.

In summary, the results from both the regression and the bootstrapping validation highlight that database server attacks are the dominant driver of financial loss in ransomware incidents, while settlement length has modest effect in the reduction of financial losses. Other socio-technical variables, such as preparedness and inter-organizational connections, contribute little explanatory power in this dataset. The findings suggest that organizations should prioritize strengthening database server security, data segregation, and backup protocols to mitigate the catastrophic impacts of ransomware. Additionally, organizations should recognize the value of coordinated incident response and post-incident recovery services and well develop incident response plans. Furthermore, the robust evidence from the bootstrapping analysis reinforces the reliability of these conclusions and demonstrates the effectiveness of the Gamma-regression framework in modeling skewed cyber-loss data.

5. Discussion and Future Work

The results provide important empirical insights into the mechanisms driving ransomware loss severity and demonstrate the value of quantitative cyber-risk modeling in technical security research. First, H1 emphasizes the influence of database server involvement on ransomware loss severity. The statistical significance of this variable highlights the central role of database servers in shaping financial outcomes and reinforces the need for prioritized protection of servers through segmentation, backup redundancy, and access-control hardening, as well as continuous monitoring for lateral movement within enterprise networks.

Regarding H3, the significant negative coefficient suggests that extended settlement period is associated with reduced financial losses. This pattern indicates that organizations benefiting from longer settlement periods may have more time to prepare negotiation strategies and implement effective mitigation measures to reduce potential losses. From a cybersecurity engineering standpoint, this highlights the importance of automated incident response systems, pre-approved recovery playbooks, and rapid decryption readiness testing to shorten response cycles without compromising long-term resilience.

H2 was not supported, as the preparedness variable was statistically insignificant in the regression model. Preparedness, operationalized through insurance coverage, did not significantly influence loss severity. This likely reflects the fact that insurance ratios do not capture underlying technical readiness, such as patching practices, endpoint protection, or offline backup quality. Similarly, H4 was not confirmed, as the number of affected entities showed no significant effect on losses. This result suggests that a simple count of affected organizations cannot capture the complexity of interorganizational dependencies, and may require more granular data, such as supply-chain topology, to capture the true impact.

These findings collectively demonstrate both the usefulness and limitations of the current dataset. While the Advisen Cyber Loss Dataset offers valuable and detailed information, its coverage is restricted to publicly reported or insured events, which may not include complex loss propagation patterns that occur within interconnected networks. For instance, the "affected entities" variable may not sufficiently capture the depth of supply-chain interdependencies or cross-organizational recovery coordination. Future work should incorporate more granular technical and organizational indicators (e.g. system topology, real-time telemetry, and incident response quality) to improve explanatory depth and extend the analysis to multi-source datasets to better support more comprehensive risk modeling.

In addition, the version in this study does not include ransomware incidents that occurred after 2020. The ransomware threat landscape has evolved considerably since the onset of the COVID-19 pandemic. Post-2020 developments, such as the emergence of more aggressive double-extortion and triple-extortion tactics, the rise of Ransomware-as-a-Service operations, and the integration of generative AI into cyberattacks, are therefore not captured in the current dataset. However, the analytical framework developed in this study remains applicable and adaptable to more recent datasets. As newer datasets become available, this methodology can be employed in future work to conduct updated analyses that reflect the latest trends in the ransomware landscape.

Methodologically, the study validates the applicability of Gamma regression with bootstrapping for cyber-loss analysis. This modeling approach effectively handles the heavy-tailed nature of ransomware data, reducing bias from extreme events while preserving interpretability. Bootstrapping further enhances robustness by confirming coefficient stability under repeated sampling, which is essential in cybersecurity datasets often characterized by limited incident reporting. Such techniques advance empirical rigor in cybersecurity research and bridge the gap between actuarial modeling and system security analytics.

To summarize, the findings not only quantify the economic impact of ransomware incidents but also provide a data-driven foundation for advancing technical cyber defense strategies. The integration of empirical loss modeling with operational cybersecurity practices can enhance predictive threat analysis, prioritize high-value targets for protection, and support the development of adaptive response mechanisms against evolving ransomware campaigns.

6. Conclusion

This study developed a data-driven framework to quantify ransomware loss severity using empirical incident data and a Gamma regression model validated through bootstrapping. By combining socio-technical variables with a statistical approach suited to positively skewed cyber-loss distributions, the analysis demonstrates that empirical modeling can enhance both academic understanding and practical defense of digital infrastructure.

The results confirm that ransomware incidents involving database server compromise are reliably associated with distinct financial impacts. This emphasizes the critical need for organizations to prioritize the protection of their information systems, particularly database servers, through robust access control, encryption, system segmentation, and timely patching of known vulnerabilities. In addition, the results reveal that shorter settlement durations are associated with reduced financial losses. This highlights the importance of well-designed incident response plans that facilitate rapid reaction and recovery. Moreover, continuous employee training, especially on social engineering tactics used by attackers, remains essential to reduce organizational exposure and enhance overall resilience.

Methodologically, this work validates the use of Gamma-based generalized linear modeling and bootstrapping as reliable tools for cybersecurity risk quantification. These techniques address the statistical challenges inherent in sparse and heavy-tailed cyber-incident datasets, offering a replicable path for empirical assessment of cyber-threat impacts that bridges data analytics and cyber defense operations.

From a technical defense perspective, the findings advocate for targeted hardening of server environments, implementation of redundant and isolated backups, and automation of recovery workflows to reduce both downtime and financial exposure. The framework can also support cybersecurity analytics by serving as a baseline for integrating AI-driven prediction or dynamic loss forecasting into security-operations platforms.

Future research should fuse this statistical foundation with machine learning based threat intelligence and real time telemetry analysis to construct adaptive, continuously learning risk models. Such integration will bridge quantitative cyber-loss modeling with active defense systems, advancing predictive resilience against the next generation of ransomware attacks.

Acknowledgements

This paper is based on parts of the author's doctoral dissertation, titled Safeguard Cyberspace in Ransomware Era: Risk Analysis & Cyber Insurance (University at Albany, 2025).

This work was made possible by the Advisen Cyber Loss Dataset. The authors thank Advisen Ltd. for providing this valuable resource.

Ethical Declaration: Ethical approval was not required.

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

References

AC Best, n.d. *Best's Market Segment Report: Ransomware and Aggregation Issues Call for New Approaches to Cyber Risk.* [Online] Available at: https://news.ambest.com/PR/PressContent.aspx?refnum=30762&altsrc=9[Accessed 6 June 2025].

Advisen Insurance Intelligence, 2015. *Cyber Risk Data Methodology for Insurance Risk Analysis.* [Online] Available at: https://www.advisenltd.com/wp-content/uploads/2015/04/cyber-risk-data-methodology-2015-04-30.pdf [Accessed 9 November 2024].

Anderson, R. et al., 2013. Measuring the Cost of Cybercrime. *The Economics of Information Security and Privacy,* pp. 265-300.

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.

Ben-Assuli, O. & Padman, R., 2020. Trajectories of Repeated Readmissions of Chronic Disease Patients: Risk Stratification, Profiling, and Prediction.. *MIS Quarterly,* 44(1), pp. 201-227.

Brewer, R., 2016. Ransomware Attacks: Detection, Prevention and Cure. *Network Security,* 2016(9), pp. 5-9.

Brown, C. et al., 2019. Accounting for Business Adaptations in Economic Disruption Models. *Journal of Infrastructure Systems,* 25(1), p. 04019001.

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.

Dekker, M. & Karsberg, C., n.d. *Technical Guideline on Incident Reporting,* s.l.: ENISA.

Dutta, K. & Perry, J., 2007. *A Tale of Tails: An Empirical Analysis of Loss Distribution Models for Estimating Operational Risk Capital,* s.l.: Federal Reserve Bank of Boston.

Edwards, B., Hofmeyr, S. & Forrest, S., 2016. Hype and Heavy Tails: A Closer Look at Data Breaches. *Journal of Cybersecurity,* 2(1), pp. 3-14.

Gordon, L. A. & Loeb, M. P. S. T., 2003. A Framework for Using Insurance for Cyber-risk Management. *Communications of the ACM,* 46(3), pp. 81-85.

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.

Harkins, M. & Freed, A. M., 2017. The Ransomware Assault on The Healthcare Sector. *JL & Cyber Warfare,* Volume 6, p. 148.

Hoferek, M. J. & Wilson, S. C., 2007. *Recovering from Database Recovery: Case Studies and The Lessons They Teach.* s.l., IEEE.

Kim, S. H. & Kwon, J., 2019. How do EHRs and a Meaningful Use Initiative Affect Breaches of Patient Information?. *Information Systems Research,* 30(4), pp. 1184-1202.

Li, W., Leung, A. & Yue, W., 2023. Where is IT in Information Security? The Interrelationship among IT Investment, Security Awareness, and Data Breaches. *MIS Quarterly,* 47(1), pp. 317-342.

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. et al., 2019. Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. *Information Systems Frontiers,* 21(5), pp. 997-1018.

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.

Okafor, C., Schorlemmer, T., Torres-Arias, S. & Davis, J., 2022. *SoK: Analysis of Software Supply Chain Security by Establishing Secure Design Properties.* s.l., ACM.

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.

Samonas, S., Dhillon, G. & Almusharraf, A., 2020. Stakeholder Perceptions of Information Security Policy: Analyzing Personal Constructs. *International Journal of Information Management,* Volume 50, pp. 144-154.

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.