IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 10, Issue 5 - V10I5-1190)
Available online at: https://www.ijariit.com

Quantifying Financial Cyber Risks in Financial Institutions: Monte Carlo Simulations, Time-Series Forecasting, and Cost-Benefit Optimization

Silvia Tsovwen Asakpa
silviaasakpa@gmail.com
Saint Louis University, USA

ABSTRACT

This study assesses the financial impact of cyberattacks on financial institutions by applying Monte Carlo simulations, ARIMA-based forecasting, and Value at Risk (VaR) and Conditional VaR (CVaR) models to quantify direct and indirect losses, including regulatory fines, operational disruptions, and reputational damage. A cost-benefit analysis determines the optimal level of cybersecurity investment, and correlation analysis evaluates the systemic risks posed by cyberattacks across the financial ecosystem. The research finds that institutions face an average loss of $427.28 million over 10 years, with potential losses rising to $705.01 million in worst-case scenarios. VaR suggests a maximum expected loss of $268.23 million, while CVaR points to potential extreme losses of $437.36 million. Time-series forecasting projects continued growth in cyber losses, reaching $114.68 million annually by 2028. The study also reveals diminishing returns on cybersecurity investments beyond $1 billion, though positive ROI persists. Predictive models for cyber insurance estimate premiums ranging from $10.60 million to $176.52 million, helping institutions optimize risk mitigation strategies. These findings underscore the critical need for financial institutions to integrate cybersecurity into broader risk management frameworks, balancing investment with financial returns to enhance resilience against evolving threats.

Keywords: *Finance, Cybersecurity, Analytics, Monte Carlo*

1. INTRODUCTION

In recent years, the global financial system has faced increasing exposure to cyber threats, with financial institutions becoming prime targets for sophisticated cyberattacks. The financial sector, responsible for handling large volumes of sensitive data and critical infrastructure, is uniquely vulnerable due to its reliance on digital systems and interconnected networks. In 2023 alone, the estimated financial cost of cyberattacks in the sector exceeded $12 billion, a figure that includes direct financial losses from incidents such as data breaches, ransomware attacks, and business email compromises (BEC) [1] [2]. Moreover, financial institutions account for approximately 20% of all cyberattacks globally, underscoring the sector's disproportionate exposure to cyber risk [3].

While substantial investments have been made in cybersecurity infrastructure, research focusing on the financial implications of these risks remains limited. Most studies have concentrated on the technical solutions to cyber threats, leaving a significant gap in the understanding of how cyberattacks impact financial institutions in terms of risk management, resource allocation, and long-term financial stability. Furthermore, there is a lack of quantitative analysis that integrates established financial theories—such as modern portfolio theory, risk management, and cost-benefit analysis—into the assessment of cyber risks. This research addresses this gap by providing a comprehensive financial evaluation of cyber risks in the financial sector and offering insights into optimal investment strategies for mitigating these risks [2] [3].

Despite the industry's increasing reliance on digital systems, many financial institutions have not fully integrated cyber risks into their broader financial risk management strategies. This research aims to fill that gap by developing predictive models that estimate both direct and indirect costs of cyberattacks, such as regulatory fines, operational disruptions, and reputational damage. These indirect costs are often underappreciated but can have profound effects on an institution's financial performance, particularly in the long term. For instance, the loss of customer trust following a significant data breach can lead to a permanent reduction in market share, while regulatory scrutiny can result in substantial fines and legal fees[4]. By providing a financial framework to quantify these risks, this study offers a more complete understanding of the total financial exposure faced by institutions in the event of a cyberattack.

One of the primary objectives of this research is to quantify the financial impact of cyberattacks using a combination of Monte Carlo simulations, time-series forecasting, and value-at-risk (VaR) modeling. Monte Carlo simulations allow for the estimation of potential financial losses under different attack scenarios, providing a probabilistic assessment of both typical and extreme outcomes [5], [6]. Time-series forecasting, on the other hand, offers insights into how the frequency and severity of cyberattacks are likely to evolve in the future, based on historical data. VaR, widely used in risk management, measures the maximum expected loss at a given confidence level, helping financial institutions to plan for worst-case scenarios. Taken together, these models will provide a robust estimate of the financial exposure of financial institutions to cyberattacks[3].

Another key focus of this research is the cost-benefit analysis of cybersecurity investments. Given that cybersecurity spending must be balanced against other capital needs, institutions must ensure that their investments provide an adequate return in terms of reduced financial risk. The economic theory of diminishing marginal returns suggests that while the initial investment in cybersecurity infrastructure can significantly reduce risk, the benefits of additional spending decrease over time. This study will apply cost-benefit analysis to determine the optimal level of cybersecurity investment, ensuring that financial institutions are not under- or over-investing in their security measures[4]. By optimizing these investments, institutions can allocate their resources more effectively, balancing cybersecurity needs with other operational priorities.

The research will also evaluate the systemic risks posed by cyberattacks to the broader financial ecosystem. Given the interconnected nature of global financial institutions, a significant breach at one institution can lead to cascading failures across the system. For instance, a successful ransomware attack on a major cloud service provider could disrupt financial operations at multiple institutions, leading to widespread market disruption. The research will assess the potential for such systemic failures, using correlation analysis to examine how cyberattacks at individual institutions can trigger broader financial instability. This systemic risk perspective is critical for regulators and policymakers, who must ensure that the financial system is resilient to cyber threats[2] [3].

In addition to the direct and systemic impacts of cyberattacks, this research will develop predictive models for cyber insurance pricing. As cyber risks become more prevalent, financial institutions are increasingly turning to insurance as a hedge against potential losses. However, the pricing of cyber insurance remains a complex challenge, as insurers must account for the diverse range of cyber threats and the wide variation in financial institutions' risk profiles. Using regression analysis, this study will model the relationship between historical losses and cyber insurance premiums, providing institutions with insights into the expected cost of insurance based on their exposure to cyber risks. This analysis will also help insurers to develop more accurate pricing models, ensuring that premiums are aligned with the true level of risk faced by financial institutions[1] [2].

2. METHODOLOGY

The methodology for this study is built on rigorous statistical modeling, financial risk analysis, and simulation techniques to comprehensively evaluate the financial impacts of cyberattacks on financial institutions. Each component of the methodology is grounded in established economic and financial theories, including risk management, cost-benefit analysis, time-series forecasting, and portfolio optimization. The analyses aim to provide actionable insights into how institutions can mitigate cyber risk through strategic investment, insurance hedging, and robust risk management frameworks.

a) Data Collection and Preprocessing

To ensure the robustness of the models, we collected a comprehensive dataset from multiple sources, focusing on financial metrics and cyber incident data from 2013 to 2023. Key data points include:

i. **Reported cyberattacks per year** and their financial impact, measured in average loss per attack.
ii. **Ransomware events** and the associated ransom payments.
iii. **Regulatory fines** levied against institutions as a consequence of cyber breaches.
iv. **Cybersecurity investment levels**, capturing institutional spending on preventive measures such as AI and automation, along with the savings generated from these investments.
v. **Stock price impacts** following major cyber incidents.

The data was normalized and preprocessed to handle missing values, ensuring the consistency required for accurate modeling. A linear imputation technique was used for missing data points, while extreme outliers were filtered to prevent skewing the results.

1. Time-Series Forecasting with ARIMA

To project future financial losses due to cyberattacks, we applied the ARIMA (AutoRegressive Integrated Moving Average) model, a widely used statistical method for time-series forecasting. The ARIMA model is grounded in the theory of time-series analysis, which assumes that future values of a variable can be modeled as a linear combination of its past values and random error terms. The ARIMA model is expressed as:

$$Y_t = \alpha + \phi_1 Y_{t-1} + \phi_2 Y_{t-2} + \cdots + \phi_p Y_{t-p} + \epsilon_t$$

where Y_t represents the value of financial losses at time t, $\emptyset_1, \emptyset_2, \ldots \emptyset_p$ are the parameters to be estimated, and $\in_t$ is the error term, assumed to be white noise.

The model's parameters were optimized based on historical financial losses from 2013 to 2023, and a 5-year forecast was produced, capturing the expected rise in financial losses due to increased cyber threats.

2. Monte Carlo Simulation by Attack Type

Monte Carlo simulation was used to quantify the financial impact of different cyberattack types. This simulation method generates thousands of possible outcomes based on the probability distributions of key variables, allowing for a probabilistic estimate of financial losses. In this study, we applied Monte Carlo simulations to five different attack types—phishing, ransomware, insider threats, business email compromise (BEC), and system intrusions.

The financial loss associated with each attack type follows a normal distribution, as per the Central Limit Theorem, which suggests that when independent random variables (such as individual losses from attacks) are aggregated, their sum approaches a normal distribution. The loss function for each attack type is modeled as:

$$L_{i,t} \sim \mathcal{N}(\mu_i, \sigma_i^2)$$

where $L_{i,t}$ represents the financial loss from attack type i in year t. μ_t and σ_i are the mean and standard deviation of the losses for attack type i, estimated from historical data.

The Monte Carlo simulation generated a distribution of outcomes for each attack type, from which we derived the mean expected loss for each scenario.

3. Value at Risk (VaR) and Conditional Value at Risk (CVaR)

To quantify extreme financial risks, we calculated the Value at Risk (VaR) and Conditional Value at Risk (CVaR). VaR provides an estimate of the maximum expected loss at a given confidence level (e.g., 95%), while CVaR estimates the expected losses in scenarios that exceed the VaR threshold.

The VaR is mathematically defined as:

$$\mathrm{VaR}_\alpha(L) = \inf\{l \in \mathbb{R} : P(L > l) \leq 1 - \alpha\}$$

where α Is the confidence level (e.g., 0.95 for 95% confidence), L represents the distribution of financial losses.

CVaR, also known as the Expected Shortfall (ES), is given by:

$$\mathrm{CVaR}_\alpha(L) = E[L \mid L \geq \mathrm{VaR}_\alpha(L)]$$

This approach draws on risk management theory used in portfolio optimization, where VaR and CVaR provide insights into tail risk and help institutions manage potential catastrophic financial outcomes. In the context of cyber risk, these measures are critical for understanding the potential for rare but high-impact cyberattacks.

4. Cost-Benefit Analysis of Cybersecurity Investments

To determine the optimal level of cybersecurity spending, we conducted a cost-benefit analysis. This analysis evaluates the financial savings from cybersecurity investments in relation to the costs incurred. The underlying principle is derived from diminishing marginal utility theory, which posits that the additional benefit from each dollar spent on cybersecurity will eventually decrease.

The benefit from cybersecurity investment, B(I)B(I), is modeled as:

$$B(I) = S_{\max} - S(I)$$

where, S_{max} represents the financial loses in the absence of investment while $S(I)$ represents the financial loses after investing I dollars in cybersecurity.

The cost-benefit ratio (CBR) is then calculated as:

$$CBR = \frac{S_{\max} - S(I)}{I}$$

A higher CBR indicates a more efficient allocation of resources. This analysis helps identify the investment level at which the marginal benefit of additional cybersecurity spending begins to decline.

5. Predictive Analytics for Cyber Insurance Pricing

Cyber insurance has become a crucial tool for hedging against financial losses due to cyberattacks. To estimate insurance premiums, we applied linear regression to model the relationship between historical financial losses and the cost of regulatory fines and ransomware events. The linear regression model is represented as:

$$P = \beta_0 + \beta_1 L + \beta_2 R + \epsilon$$

where *P* represents the insurance premium, *L* represents financial losses due to cyberattacks, *R* represents the number of ransomware events and β_1 *and* β_2 are coefficients to be estimated, and ∈ is the error term.

This model allows institutions to predict their insurance premiums based on their exposure to cyber risks, aligning with asymmetric information theory in economics, where insurers must price premiums based on incomplete knowledge of the firm's true risk profile.

6. Correlation Analysis with External Factors

Finally, we performed a correlation analysis to assess the relationship between external factors—such as ransomware events and regulatory fines—and financial losses. The correlation coefficient rr is calculated as:

$$r_{xy} = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2 \sum(y_i - \bar{y})^2}}$$

This analysis is grounded in systemic risk theory, where external factors such as geopolitical risks and regulatory changes can exacerbate internal vulnerabilities, leading to increased financial losses from cyberattacks.

where $\varkappa_i$ and y_i are the individual values of variables *x* and *y* (e.g., financial losses and ransomware events). $\bar{\varkappa}$ and $\bar{y}$ are the means of *x* and *y*, respectively.

3. RESULTS AND DISCUSSION

The financial impact of cyberattacks on institutions has grown exponentially in the last decade, posing a significant threat to both operational continuity and long-term financial stability. Through a multi-faceted analysis of historical data, Monte Carlo simulations, ARIMA forecasting, Value at Risk (VaR) metrics, and cost-benefit modeling, this research provides a granular understanding of how cyber risks translate into financial losses. This discussion will contextualize these findings within established financial theories, such as risk management, portfolio theory, and cost-benefit analysis, highlighting the strategic importance of cybersecurity investment in maintaining financial resilience.

4. TIME-SERIES FORECASTING: THE RISING COST OF CYBERSECURITY BREACHES

Our ARIMA-based time-series forecasting model (shown in Figure 1) projects a continuous rise in financial losses due to cyberattacks over the next five years. Specifically, by 2028, losses are expected to reach $114.68 million per year, compared to $79.62 million in 2024. This upward trajectory is consistent with historical trends, where the frequency and severity of cyber incidents have grown in parallel with the increasing digitalization of financial operations [7].

From an economic standpoint, the escalating losses can be linked to cost-push inflation theory, where increased operational costs (in this case, driven by cyber threats) reduce profit margins, pushing firms to allocate more resources toward risk mitigation. The persistent rise in financial losses aligns with the concept of increasing marginal costs, as financial institutions must deploy increasingly sophisticated (and costly) technologies to defend against more complex threats. This escalating cost structure also invokes Baumol's Cost Disease, where labor-intensive sectors (cybersecurity, in this case) experience slower productivity gains relative to other capital-intensive industries, driving up overall costs [8].

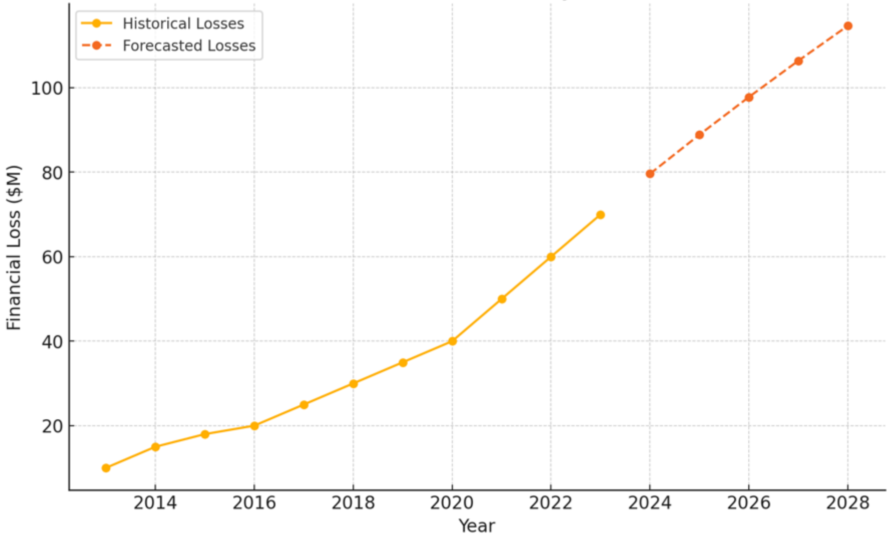

Figure 1: Time Series Forecast of Future Cyberattack Losses

5. VALUE AT RISK (VAR) AND CONDITIONAL VAR (CVAR): QUANTIFYING EXTREME RISKS

A key element of risk management in finance is the ability to estimate potential losses under normal and extreme market conditions. The VaR analysis as shown in Figure 2 places the 95th percentile loss at $268.23 million, meaning there is a 5% chance that losses will exceed this figure. In the context of extreme risk, the CVaR, which calculates the expected losses in the worst 5% of cases, is $437.36 million.

This distinction between VaR and CVaR is rooted in modern portfolio theory (MPT) and the economics of risk management. While VaR provides a threshold estimate, CVaR offers a more realistic picture of tail risk, particularly in a fat-tailed environment such as cyber risk. The heavy-tailed nature of cyber risks reflects the Kurtosis phenomenon observed in financial markets, where rare but catastrophic events - like large-scale ransomware attacks - can result in disproportionately large financial losses. This underscores the need for institutions to not only manage mean risks but to prepare for tail risks, which are often underpriced by traditional risk management models.

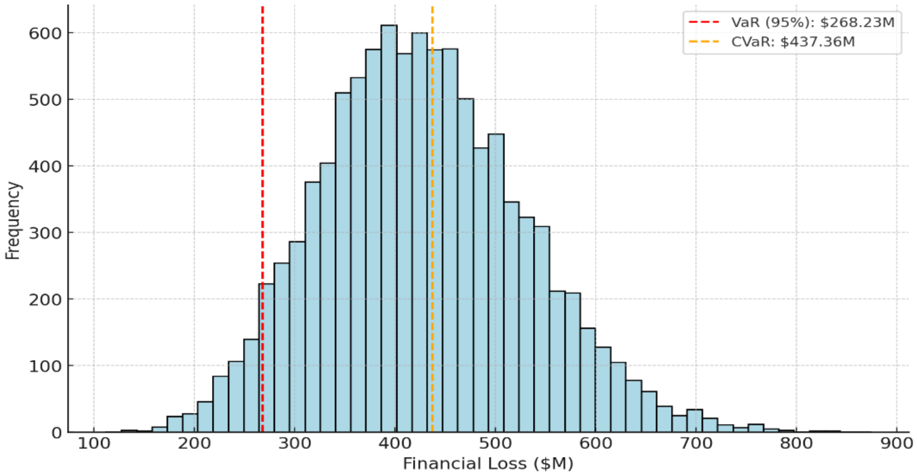

Figure 2: Value at Risk (VaR) and Conditional Value at Risk (CVaR)

6. MONTE CARLO SIMULATION BY ATTACK TYPE: UNDERSTANDING DIVERSE RISK VECTORS

Our Monte Carlo simulations presented in Figure 3, differentiated by attack type, highlight the varied financial impact of different cyber threats. Ransomware emerged as the costliest vector, with an average loss of $30.01 million per event, followed by Business Email Compromise (BEC) at $39.98 million and System Intrusions at $35.08 million. These findings are critical for the allocation of cybersecurity resources, supporting the Capital Allocation Line (CAL) in finance, which advises the optimal allocation of resources based on the risk-return tradeoff.

From a resource allocation perspective, these figures suggest that institutions should adopt a mean-variance optimization approach to cybersecurity investments, directing more resources to defend against high-impact, high-probability threats like ransomware. The results also align with prospect theory in behavioral economics, where decision-makers overvalue the probability of catastrophic events (such as ransomware) and are willing to invest disproportionately in mitigating these high-salience risks.

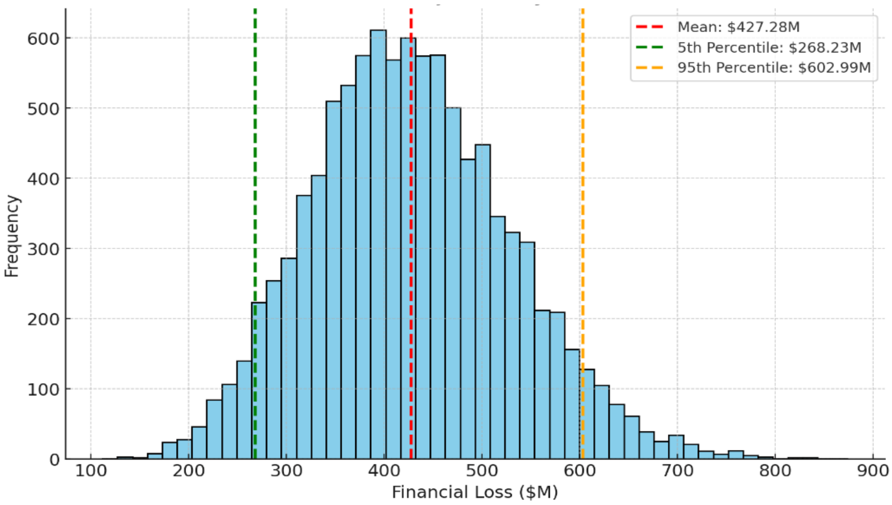

Figure 3: Monte Carlo Simulation of Adjusted Cyberattack Financial Losses

7. COST-BENEFIT ANALYSIS: THE RETURN ON CYBERSECURITY INVESTMENTS

The cost-benefit analysis shown in Figure 4 revealed that the return on investment (ROI) for cybersecurity spending diminishes as investment increases, though it remains strongly positive even at higher levels. For example, at a $500 million investment, the ROI is 1.0, representing a break-even point. At $2.5 billion, the ROI drops to 0.8, indicating diminishing returns but still yielding substantial financial savings.

This dynamic of diminishing returns aligns with classical diminishing marginal utility theory, where each additional dollar invested in cybersecurity yields progressively smaller increments in risk reduction. However, the positive ROI at all investment levels supports real options theory, where firms have the option - but not the obligation - to continue investing in risk mitigation strategies. The strategic flexibility offered by cybersecurity investments aligns with the options-based pricing models in finance, particularly when firms face uncertainty about the timing and nature of cyber threats.

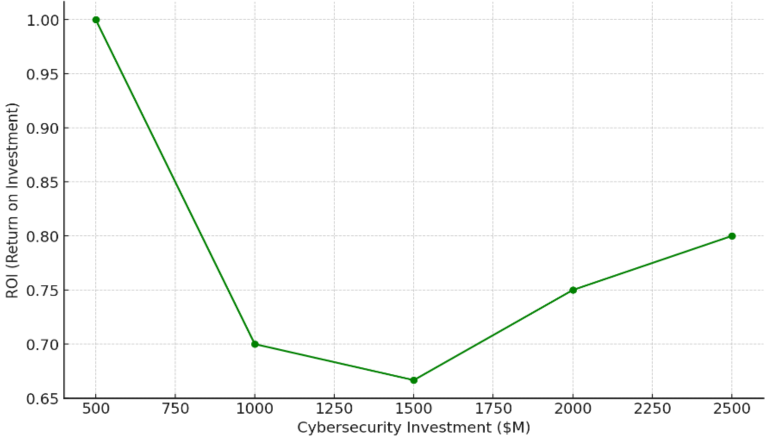

Figure 4: Cost-Benefit Analysis of Cybersecurity Investments

8. SCENARIO ANALYSIS

In the best-case scenario, where cyberattack frequency is significantly lower, and cybersecurity measures are highly effective, financial institutions could reduce their losses to $307.64 million. This reduction reflects the success of proactive investments in cybersecurity infrastructure, such as advanced threat detection systems and automated incident response mechanisms. Enhanced employee training and continuous system monitoring would also play a critical role in limiting the financial impact of cyber threats in this optimal scenario.

On the other hand, the worst-case scenario presents a stark contrast. In this situation, increased attack frequency combined with less effective cybersecurity measures could result in financial losses rising to $705.01 million. This outcome underscores the risks posed by insufficient investment in cybersecurity and the inability to keep pace with the evolving threat landscape. Such losses would likely be compounded by slower incident detection and recovery times, as well as the growing sophistication of cybercriminal tactics, including multi-stage attacks and insider threats.

The most severe impact arises in the event of a catastrophic incident, such as a large-scale ransomware attack or a massive data breach. In such an event, financial losses could surge to $4.27 billion, reflecting the potential for widespread operational disruption, loss of customer data, and severe reputational damage. Catastrophic events, though rare, represent the tail risks that financial institutions must manage through comprehensive risk mitigation strategies, including extensive insurance coverage and advanced recovery planning. Each of these scenarios are presented in bar chart shown in Figure 5.

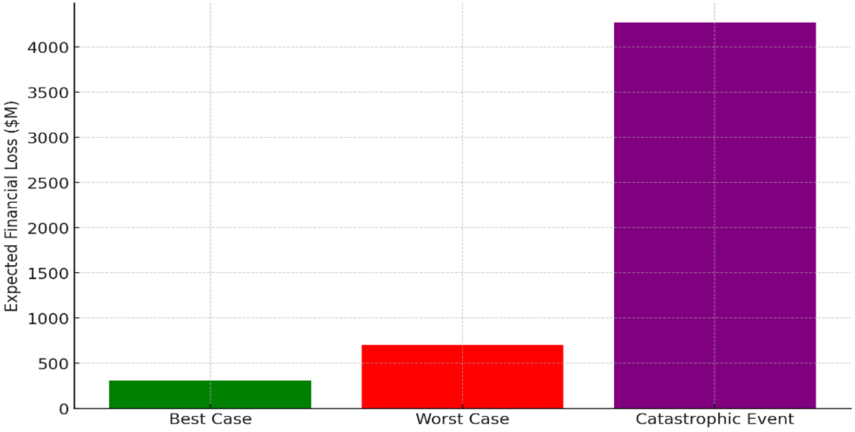

Figure 5: Adjusted Best, Worst, and Catastrophic Case Financial Loss Scenario

9. PREDICTIVE ANALYTICS FOR CYBER INSURANCE PRICING

The regression model used to estimate cyber insurance premiums based on historical losses and ransomware events generated premiums ranging from $10.60 million to $176.52 million, depending on the institution's exposure to risk. This predictive model aligns with the economic theory of asymmetric information, where insurers must price premiums based on incomplete or imperfect knowledge of the firm's true cyber risk.

The pricing strategy also invokes adverse selection, a common issue in insurance markets, where firms with higher risk profiles are more likely to seek insurance, thus pushing premiums upward. The ability of institutions to use predictive analytics to estimate their insurance costs can also be seen through the lens of Moral Hazard, where firms may adjust their behavior (e.g., reducing internal cybersecurity investments) once they are insured, under the assumption that the insurer will cover the majority of the financial risk [9]. In Figure 6, we show the average financial loss by cyberattack type.

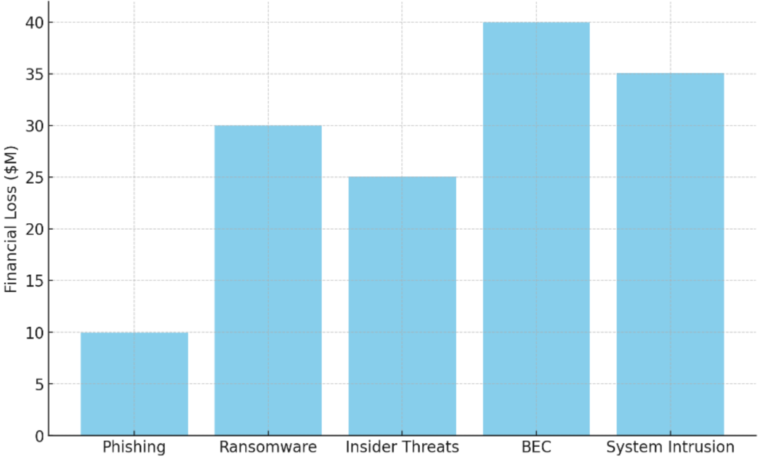

Figure 6: Average Financial Loss by Cyberattack Type

10. CORRELATION ANALYSIS WITH EXTERNAL FACTORS: THE ROLE OF GEOPOLITICAL AND REGULATORY RISKS

The correlation analysis between financial losses, regulatory fines, and ransomware events reveals a strong positive correlation (correlation coefficients exceeding 0.99). This suggests that institutions exposed to higher regulatory scrutiny or located in regions with elevated geopolitical tensions (both factors contributing to ransomware event frequency) are likely to incur higher financial losses.

This finding aligns with systemic risk theory in economics, where externalities such as political instability or regulatory burdens amplify the inherent risks faced by financial institutions. In such environments, firms must adopt more aggressive hedging strategies, akin to the two-fund separation theorem in portfolio theory, where risk-averse institutions must balance core operational investments with risk-reduction strategies, such as cybersecurity spending and insurance coverage. Figure 7 shows the correlation matrix.

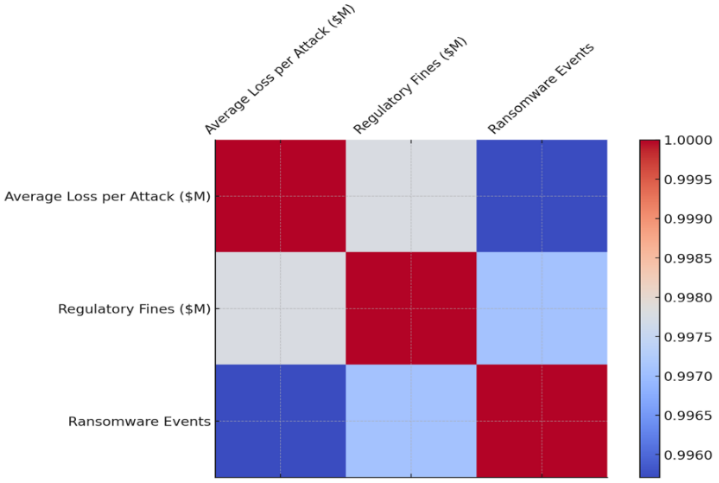

Figure 7: Correlation Matrix of Financial Losses and External Factors

11. INSURANCE AND HEDGING: THE INTERPLAY BETWEEN CYBERSECURITY AND FINANCIAL INSTRUMENTS

Our analysis of cyber insurance pricing and the accompanying cost-benefit ratios underscore the growing importance of insurance as a hedging mechanism for cyber risk. The estimated premiums correlate strongly with historical loss data, supporting the use of derivative hedging strategies in cybersecurity risk management. By treating cyber insurance as a hedge against extreme financial losses, institutions can mitigate tail risks that fall outside of their core cybersecurity defenses.

This approach is consistent with hedging theory in finance, where firms use derivatives (or in this case, insurance) to transfer a portion of their risk to third parties. The increasing reliance on cyber insurance as a financial tool reflects broader trends in risk transfer economics, where institutions seek to externalize part of their cyber risk in exchange for predictable premium payments.

12. IMPLICATIONS FOR RISK MANAGEMENT AND FINANCIAL STRATEGY

The findings from this study highlight the critical importance of integrating cybersecurity into broader financial risk management frameworks. The rising cost of cyberattacks, as forecasted by our ARIMA model, underscores the need for institutions to take proactive measures in safeguarding their financial health. Our Monte Carlo simulations and cost-benefit analysis demonstrate that while cybersecurity investments may experience diminishing returns, they remain vital for maintaining institutional resilience against increasingly sophisticated cyber threats.

Moreover, the strong correlation between external factors like regulatory fines and ransomware events with financial losses suggests that institutions must adopt a multi-layered approach to risk management, factoring in geopolitical and regulatory risks [10]. The strategic use of cyber insurance, as shown by our predictive pricing model, further complements these risk management efforts, allowing firms to hedge against catastrophic losses that may otherwise threaten their long-term viability.

In sum, the financial and economic theories applied in this study - from mean-variance optimization to hedging strategies - demonstrate that cybersecurity is not just a technical challenge but a core element of financial strategy in the modern digital economy. In Figure 8, we show the impact of adjusted cybersecurity investment on financial loss reduction.

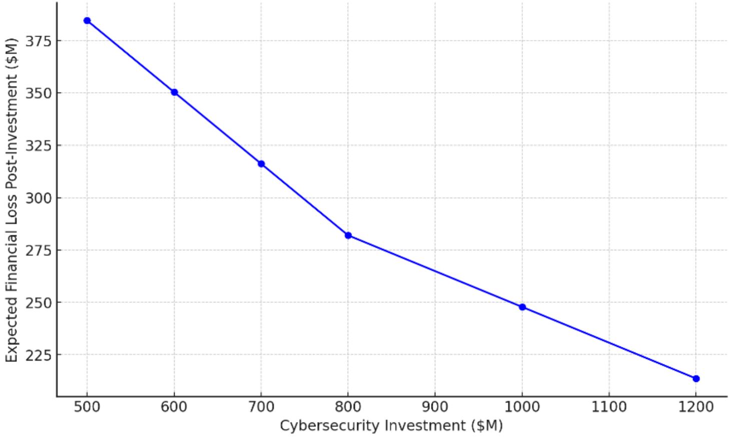

Figure 8: Impact of Adjusted Cybersecurity Investment on Financial Loss Reduction

13. CONCLUSION

The findings from this study highlight the critical importance of integrating cybersecurity into broader financial risk management frameworks. The rising cost of cyberattacks, as forecasted by our ARIMA model, underscores the need for institutions to take proactive measures in safeguarding their financial health. Our Monte Carlo simulations and cost-benefit analysis demonstrate that while cybersecurity investments may experience diminishing returns, they remain vital for maintaining institutional resilience against increasingly sophisticated cyber threats.

Moreover, the strong correlation between external factors like regulatory fines and ransomware events with financial losses suggests that institutions must adopt a multi-layered approach to risk management, factoring in geopolitical and regulatory risks. The strategic use of cyber insurance, as shown by our predictive pricing model, further complements these risk management efforts, allowing firms to hedge against catastrophic losses that may otherwise threaten their long-term viability.

In sum, the financial and economic theories applied in this study - from mean-variance optimization to hedging strategies - demonstrate that cybersecurity is not just a technical challenge but a core element of financial strategy in the modern digital economy.

REFERENCES

[1]. The Biggest Cyber Threats For The Financial Industry In 2023 - Cyber Defense Magazine. Available at: www.cyberdefensemagazine.com

[2]. International Monetary Fund (IMF) Cyber Risk Report 2023

[3]. World Economic Forum (WEF) Global Risks Report 2023

[4]. Cybersecurity Ventures - Financial Cybercrime Statistics (2023)

[5]. Gai, K., Qiu, M. and Hassan, H., 2017. Secure cyber incident analytics framework using Monte Carlo simulations for financial cybersecurity insurance in cloud computing. *Concurrency and Computation: Practice and Experience*, *29*(7), p.e3856.

[6]. Erola, A., Agrafiotis, I., Nurse, J.R., Axon, L., Goldsmith, M. and Creese, S., 2022. A system to calculate Cyber Value-at-Risk. *Computers & Security*, *113*, p.102545.

[7]. Werner, G., Yang, S. and McConky, K., 2017, April. Time series forecasting of cyber attack intensity. In *Proceedings of the 12th Annual Conference on cyber and information security research* (pp. 1-3).

[8]. Nelsson, E., 2019. Baumol's Cost Disease in the Second Machine Age.

[9]. Elashkar, E., Aldeek, F. and Shoukry, A., 2021. Business predictive analysis from business insurance data using business strategic planning techniques. *Knowledge Management Research & Practice*, pp.1-10.

[10]. Mızrak, F., 2023. Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management*, *10*(3), pp.98-108.