International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V4I3P113
Eureka Vision Publication | Volume 4, Issue 3, 124-133, 2023

Original Article

Cyber Insurance Evolution: Addressing Ransomware and Supply Chain Risks

Komal Manohar Tekale
Independent Researcher, USA.

Abstract - The market of cyber insurance has considerably changed due to the rise of the prevalence of ransomware and supply chain cyberattacks. Cyber insurance, which was initially a niche financial tool, has since been a necessary risk transfer tool to businesses in the new digital ecosystem. The paper will focus on the history of cyber insurance with regards to two imminent risks, i.e., ransomware and the compromise of the supply chain. Ransomware attacks have become more numerous and sophisticated due to the presence of organized networks of cybercriminals as part of which they are carried out with the help of sophisticated encryption, affiliate business model and payment in cryptocurrency. Equally, the resiliency of supply chain risks has been characterized by the increasing dependency on third-party suppliers, cloud service providers and software dependencies, which weigh the system vulnerability. In this paper, I will begin by discussing the conceptual framework of cyber insurance, its application as a means of financial recovery and as an incentive to be more secure. The cyber insurance (unlike traditional one), will be forced to continuously incorporate itself into the changing technological environment, regulatory forces, and the constantly varied threat environment. In a bid to remain solvent, insurers are heading towards dynamic risk assessment, actuarial models and real time threat intelligence. The paper describes how ransomware has led to reshaping the policy architecture by insurers. Coverage limitations, higher premiums, exclusion, and proactive requirements such as mandatory multi-factor authentication (MFA), endpoint detection and response (EDR) systems have also been covered. Similarly, cases of breaches of the supply chain, the most notable, SolarWinds breach and Kasey ransomware attack, are demonstrations of the devastating character of systemic cyber risk. These incidents underscore the difficulty of the modelling of correlated risks when a single compromise is being experienced by thousands of insured entities. In some respects a literature review points us to how academia, industry and regulators have been in some combination affecting cyber insurance.

A literature of scholars has shown a flaw of inefficiency with the actuarial models due to lack of historical information and the uncertainty surrounding threat agents. Reportedly, according to industry readings, claims ratios are on the steep climb, and the application of exclusions is taken in respect of the cyber activities sponsored by the state. The regulators have also focused on resilience, and insurers must change policy language and be financially solvent against accumulated losses. The approach that is advanced in this paper establishes a hybrid framework in responding ransomware and supply chain risks in cyber insurance. It combines actuarial modeling, threat intelligence that is qualitative and systemic risk simulation. Our Bayesian inference models are designed to estimate the probability of ransomware claims and Monte Carlo models are used to model dependencies in the supply chain. There is a multi-layered architecture outlined that connects security controls, design of insurance policies and evaluation of claims. The results are that the application of the proactive security requirements in cyber insurance policies is significant in reducing the overall claim rates. In addition, systemic supply chain risk models indicate that reinsurance system and risk sharing among the insurers should be formed in order to minimize the catastrophic exposures. Flowcharts and mathematical form are provided to show the interaction of insurance risks pools, insured companies and risk threats. As mentioned in the discussion the future of cyber insurance does not lie merely in indemnification but also in active co-operation in cyber risk management. Constant watch is becoming in their direction, and the artificial intelligence and the blockchain-based claims verification will be used. They arrive at the conclusion that in the event of improved integration of technology, harmonization of regulations and systemic resiliency modelling, cyber insurance will be a driving force of digital trust.

Keywords - Cyber Insurance, Ransomware, Supply Chain Risk, Cybersecurity, Systemic Risk, Actuarial Modeling, Risk Transfer, Monte Carlo Simulation.

1. Introduction

1.1. Background

Such a radical change has happened in the digital economy over the past 10 years, because it is a lot more dependent on interconnected information systems, cloud providers and software providers. These technological advances enable organizations to spread their operations and increase efficiency and deliver services to the global market better than ever. In the process, they carry with them intricate cyber exposures, as interdependences create points that threats can be transmitted extremely quickly through networks and supply chains. Cyber attacks such as ransomwares, phishing attacks, and advanced

persistent threats take advantage of these digital links, and in most instances, the cyber attacks are not targeted at a particular firm but entire ecosystems of interconnected entities. [1-3] This has seen cyber insurance becoming a financial instrument necessary to help move and cover the financial consequences of such incidences to handle the losses incurred due to data breaches, business-disruption costs, and penalties. Unlike traditional lines of insurance, though, cyber risk is indeed a non-stationary event: the frequency, scope, and quality of the breaches alter each time a new technology is incorporated in such a way the method of attacks does. This dynamism exerts stronger actuarial hypotheses by historic data and comparatively consistent risk distributions and imposes insurance requirements on insurers to devise more complicated and responsive underwriting, prices and portfolio management strategies. The interdependence inherent in technology innovation, evolving threats, and regulatory pressures, in its turn, can be interpreted to establish efficient cyber insurance systems that can not only offer financial compensation but give an incentive to implement efficient cybersecurity practices in every business sector.

1.2. Evolution of Cyber Insurance

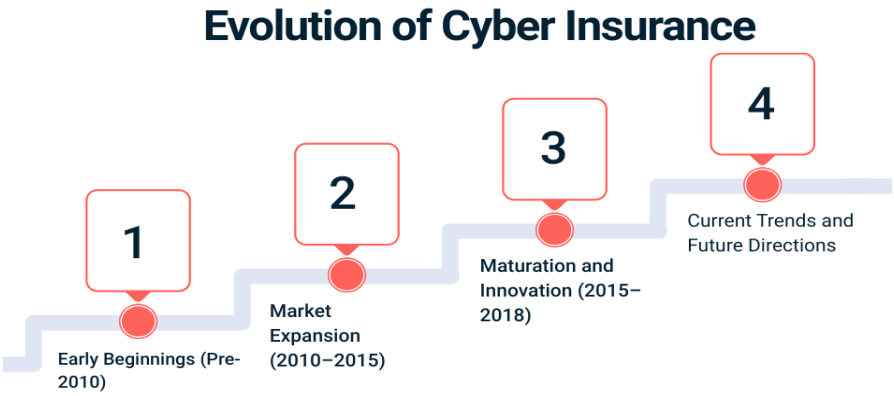

Figure 1. Evolution of Cyber Insurance

- **Early Beginnings (Pre-2010):** Historically, cyber insurance was launched towards the end of the 1990s and the early 2000s and was aimed at a niche insurance product at technology firms. . Initial policies were narrow, and they normally addressed the risk of loss of data, or failure in the network. Losses related to data loss, business interruption and third-party liability in case of security meant were usually covered. Nevertheless, the absence of historical data on losses, as well as the limited knowledge on cyber risks among companies, limited the development of the market. Traditional lines of insurance, including errors-and-omissions or general liability were generally used to underwrite policies, but each of them fell short of the distinctive features of cyber threats.
- **Market Expansion (2010–2015):** Cyber insurance: The adoption of cyber insurance in 2010-2015 started to expand into other industries, alongside the rise in the occurrence and severity of data breaches and high-profile ransomware attacks. Underwriters started to create specialized cyber products, with more comprehensive underwriting requirements and options of cover. At this time, there was an emergence of actuarial models using both historical breach data and scenario-based actuarial models though data scarcity was a problem. An increased attacker surface presented by cloud computing, mobile devices and third party vendors led insurers to create policy provisions, like business-interruption coverage, regulatory fines, and incident response services.
- **Maturation and Innovation (2015–2018):** Since 2015, cyber insurance became a more advanced and inseparable part of enterprise risk management. The insurers started adopting hybrid models of modeling their policies based on statistical analysis, scenario simulation and expert judgment to get an accurate pricing. The conditions of coverage became more Rudimed, and the ransomware, social engineering fraud and even supply chain risks are accepted as the cyber threat increased and became more and more sophisticated. The regulatory trends such as the GDPR by the EU or NIS Directive also influence policy design, introducing a series of stricter requirements of notice of breach and fines. By the end of this period, cyber insurance started to be regarded as a product that can not only turn financial risk into a viable product, but also help to encourage better cybersecurity performance, here incident report, and help organizations become sustainable.
- **Current Trends and Future Directions:** The development of cyber insurance is dynamic and continues towards real-time risk monitoring, AI-based underwriting and adjacency to cybersecurity systems. The insurers are placing greater demands on the preventive services, ongoing assessment of the client security posture and the option of dynamically priced according to the threat intelligence.The developments to come are expected to emphasize the systemic risks, including the dependence on the supply chain and correlated cyber events, and the implementation of new technology, including blockchain-based claims verification and other automated smart contracts that would enhance transparency and efficiency.

1.3. Addressing Ransomware and Supply Chain Risks

One of the most important threats to the modern cyber insurance is ransomware and supply chain risk as one of the most influential dangers to determine the current state of the cyber insurance market. [4,5] The frequency and severity of Ransomware attacks now facilitated by advanced malware or via the Ransomware-as-a-Service (RaaS) framework has increased, and organizations in all industries, such as healthcare, finance, manufacturing, and critical infrastructure, have become targets. Such attacks usually encrypt valuable data and require financial settlements, which cause a short-term operational outage and could cause a loss of reputation in the long term. The ransomware risk is dynamic, unreported, and varies, which presents unique challenges to insurers because it is difficult to model, and the impact of a ransom holds no standardized solution and is impacted by the recovery costs along with business-interruption. To implement effective risk assessment, therefore, hybrid actuarial models have to be used, one that integrates past claims data, expert judgement and current threat intelligence to predict expected losses and extreme tail events. Supply chain cyber risk adds on to this predicament as more and more companies are turning to third-party vendors, cloud platforms, and software platforms to transact their business. A breach or hack of one of the supplier systems can propagate throughout the network of the dependent companies leading to correlated losses, which will impact all insured parties simultaneously.

A 2017 incident involving the NotPetya outbreak is a well-publicized demonstration of the ripple-out of supply chain breaches, which illustrates the inability of the decades-long firm-centric underwriting mentality to enable the construction of systemic exposures. Insurers are doing things to ensure that they incorporate in portfolio risk assessment supply chain dependency analysis, scenario based stress testing and network modelling. This lessening of ransomware, supply chain dangers, requires a combination of preventive administration, adaptable underwriting and policy-making. The insurers are driving clients towards compulsory security controls, regular vendor audits and tolerating business continuity planning. Such policy structures can comprise of ransomware-specific endorsements, limits applied on coverage due to systemic failures on their supply chain, and conditional provisions involved with cybersecurity hygiene. Together as a combination of strategies, the insurers can not only help to spread financial risk but also actively contribute to strengthening organizational capabilities, to make the coverage fit the changing threat landscape and decrease the risks of large-scale cyber activities.

2. Literature Survey

2.1. Cyber Insurance Foundations

In this period of 2010-2018, the body of literature in cyber-insurance converged on three common themes; the lack of past loss data, pricing and actuarial difficulties, and contract design to address moral hazard and accumulation risk. [6-9] Early empirical and theoretical practice recorded breach-loss data were sparse and homogeneous (different definitions of breach, many minor incidences with occasional major ones), such that standard frequency-severity actuarial models failed to work, and so extensive use was made of scenario analysis and professional judgment. This led researchers and practitioners to focus on the hybrid solutions - involving econometric loss modelling, scenario/stress testing, and exposure-based underwriting - and to require better data sharing and standardisation. It was also studied in the literature that principal agency problems (insureds not spending adequately to protect themselves against cyber-attacks when they have coverage), and ways the terms of the policy (deductibles, co-insurance, security requirements, and exclusions) might address moral hazard. Lastly, the actuaries and regulators highlighting systemic accumulation risk (a company at risk due to an aggregate shared software/platform failure) as a fundamental issue highlighted how a lack of traditional line-by-line underwriting was inappropriate to measure. These themes are being encapsulated by interdisciplinary actuarial reviews and industry reports which emphasize on both methodological promise and a significant practical limitation.

2.2. Ransomware Risk Studies

Since about 2015–2018 ransomware has become an established force in academic and industry research as a prevalent cause of severity of cyber-losses, and researchers began to measure the behaviours of attackers, incentives around ransom, and insurers at risk. Surveys of the industry and filed reports of the time revealed that organizations commonly tend to evaluate the immediate ransom price against that of business-interruption and that of restoration timeframes; numerous ransom payments occurred due to the fact it was cost-effective to restore in a brief span, however the payment could and did not imply decryption and that they might trigger follow-up extortion after. Practitioner papers and scholarly studies analysed the ecosystem of ransomware-as-a-service (RaaS) and identified how commoditization has reduced the entry barriers of attackers and raised the number of attacks. The studies involving insurers also reflected a case of changing underwriting, i.e., stricter controls, specific endorsements of ransomware, and consistently surging premiums because of rising claims. Notably, initial empirical studies noted measurement issues (underreporting of payments, widespread losses between property, business interruption, forensic costs) and regulatory/legal issues (legality/OFAC risk to the extent such payments are made to sanctioned entities). These studies became the foundation of subsequent policy modification and intensive underwriting that ensued.

2.3. Supply Chain Risk Research

A 2013–2018 supply-chain cyber risk research study changed the discussion of firm-level breaches to contagion on a system-level. NotPetya/Medoc compromise and the 2017 increase of software-update supply-chain attacks demonstrated that a compromise one vendor initially may extend globally through customers and partners, causing disproportionately-vast losses.

Empirical studies - such as recent macro-level studies - report effects of amplification: downstream customers tend to experience more and more enduring revenue and profit losses compared to the supplier directly affected, in particular where customers have no alternative suppliers or buffers against shocks. Researchers simulated inter-firm exposure networks and demonstrated how concentration (a small number of large suppliers or cloud providers) and shared dependencies on third-party nodes in turn give rise to the single-point-of-failure relationships which cannot be swept out via normal portfolio diversification strategies. These articles combine event-based case studies (e.g., the effect of NotPetya on shipping, logistics, and manufacturing) with mathematical network perspectives to demonstrate that supply-chain events have a series of operational and financial impacts, which are difficult to insure and necessitate intersectoral effort to reduce the risk of impact.

2.4. Regulatory Perspectives

The regulatory environment was developing at a high rate between 2016 and 2018, especially in Europe. The GDPR (adopted 2016 and is enforceable May 25, 2018) made the incident of breach reporting and liability more heavily addressed (with heavy imposition of fines and enhanced data-subject rights) - which has a material impact on the cost of breaches, and hence insurability. The (original) NIS Directive (2016) at the EU level began to outline the nature of cybersecurity about critical-infrastructure and cooperation across borders; later versions and national adaptations prioritized incident-reporting and resiliency in essential-services. Although federal specific regulation of cyber-insurance was limited in 20102018 in the U.S., financial-sector direction and subsequent Treasury/OFAC factors brought up compliance issues related to ransom payments (sanctions risk) and a third-party payment. Insurance regulators (state and international organizations) started to pay more attention to insurer solvency, concentration risk, and disclosure - promoting data gathering (voluntary supplements and questionnaires), and more intensive monitoring of cyber product conditions. All these regulatory steps brought together heightened transparency of cyber attacks, adjusted the sizes of losses through fines and reputational consequences, and complicated underwriting mechanisms through legal and regulatory systems.

2.5. Gaps Identified

In reviews and sector studies up to 2018, there was concurring identification of a series of chronic research and practice gaps. First, actuaries and modelers did not have high-quality and standardized loss data and telemetry in real-time to support granular pricing - the empirical inference was curtailed by event disclosure behavior and non-homogeneous policy forms. Second, there were systemic and correlated risks (supply-chain cascades, cloud/provider concentration, widespread vulnerabilities) that were ill-quantifiable: network contagion models were workable, but data-intensive and hard to test with the few extreme events. Third, there was dynamic attacker behavior (RaaS, evolving extortion tactics) and the behavioral feedback between insurer behaviour (coverage limits, ransom facilitation) and criminal incentives, which were in early development phases, necessitated game theorizing and behavioural modeling. Lastly, regulatory fragmentation and uncertain legal exposure (e.g. cross-border notification, risk of sanction, etc.) complicate allocation of loss and reinsurance design. The literature demanded organized public/private data sharing, unified policy conditions, frameworks of accumulation risk stress-testing, and investment in models to integrate both network science, economics, and operational telemetry a research agenda that is still underway as these gaps directly limit robust actuary practice and market stability.

3. Methodology

3.1. Proposed Framework

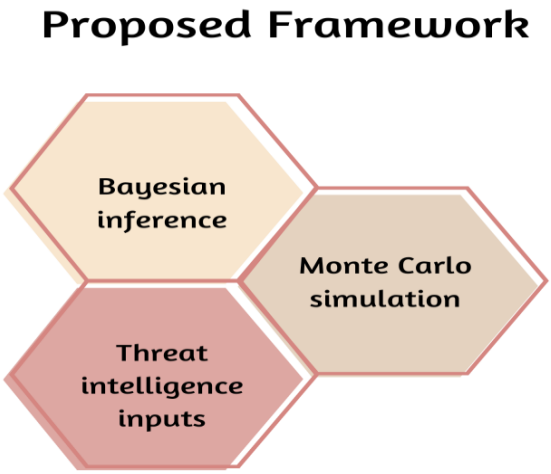

Figure 2. Proposed Framework

- **Bayesian Inference:** A Bayesian inference provides a systematic mechanism to revise cyber risk models with the coming up of new evidence. [10-12] Prior distributions may take the form of historical loss information, expert

opinion or industry values in the context of cyber insurance and enterprise risk assessment. The posterior distributions update as new incident statistics, breach reports or insurers claims become known to update the picture to the latest state of knowledge. This process of iterative learning is particularly useful in cybersecurity where actuarial assumptions based on the current situation cannot be made due to a lack of data and the dynamism of the threats. Bayesian approaches offer a clearer way to constantly update the estimation of probabilities of cyber threats and cyber losses by measuring the uncertainty and using the professional opinion and the empirically obtained data.

- **Monte Carlo Simulation:** Monte Carlo simulation is the complement of Bayesian modeling that interprets the probabilistic assumptions into simulated results that are a reflection of the entire possibility of losses. This is repeated sampling of the distributions of the threat likelihood, breach severity and systemic dependencies in cyber risk to produce thousands of loss cases. Probability distribution of the aggregate losses are the output, and can be used to estimate Value-at-Risk (VaR) or Tail-Value-at-Risk (TVaR) as used by insurers and risk managers. With this technique, the analysts can examine both tail risks and tail events as well as anticipated losses, which are important topics in determining the capital sufficiency requirement, structuring reinsurance contracts, and stress testing systemic exposures.
- **Threat Intelligence Inputs:** Bayesian and Monte Carlo models rely greatly on the quality of their inputs and this is where real time threat intelligence is most vital. Models can be dynamically configured to incorporate the new threats (indicators of compromise (IoCs), malware family feeds, vulnerability disclosure information, attacker tactics) to keep up with the dynamic threat environment. E.g. when intelligence suggests a significant increase in ransomware attacks on particular sectors, Bayesian models can have prior probabilities changed upwards and Monte Carlo can put higher weight on such events. Threat intelligence in this manner provides the balance between the non-adversarial, static actuarial, and the dynamic, adversarial cyber risk.

3.2. Mathematical Model

The mathematical model suggested here relies on a Bayesian updating model to compute the likelihood of a claim due to ransomware, which is:

$$P(R) = \frac{\alpha + X}{\alpha + \beta + N}$$

In which (R) is the probability of a ransomware claim, α and β are the parameters of the prior distribution, xcan be seen as the actual ransomware incidents, and 2n as the number of insured firms. This model takes the form of a Beta-Binomial framework that is highly effective in using both the historical information and expert judgment of risk estimation. The initial beliefs concerning the risk of ransomware (e.g., based on a compilation of industry-wide losses or on actuarial experience) are represented by the previous parameters and β loudly, and the actual incidences Xamong the insureds privatize this belief. This posterior probability ( ), where is more information-driven with more claims, can therefore allow insurers to keep refining their knowledge on ransomware frequency. It should also be noted that, unlike Bayesian updating, which is a rigorous method of estimating the probability of personal instances of ransomware, cyber risk is not limited to single instances.

Of special interest is systemic exposure, particularly, via correlated risks in relation to supply chains that consist of a single vulnerability that may come into place, including an attacked software update, a cloud service outage, or even with a popular zero-day vulnerability that causes a simultaneous claim by multiple insureds. To acquire this systemic aspect Monte Carlo simulation is done in parallel. The model determines how supply chain dependencies can enhance aggregate losses by generating thousands of artificial situations of events of correlated events, and colliding with the clusters of tail-risk which are not visible when the marginal claim distributions are used on its own. This hybrid system therefore integrates Bayesian inference to revise the probability of events with Monte Carlo simulation to stress systemic interactions as a way to provide insurers a more holistic and more resilient ransomware and supply chain cyber risk modeling ecosystem.

3.3. Flowchart of Cyber Insurance Model

- **Threat Intelligence Input:** It begins with ingesting live threat intelligence feeds that provide intelligence regarding new vectors of attack, vulnerability announcements, and attack schemes. [13-15] It is these inputs that ensure that the evaluations of the risks are not solely dependent on the past events but the present and future indications as well. As an example, underwriting assumptions and premiums can be made based on intelligence related to increasing ransomware-as-a-service assaults on the healthcare sector.
- **Actuarial Modeling:** After collection of intelligence, actuarial models are then used to convert incident probability into estimations of risk, which can be measured. The actuarial step involves measurement of both the expected and extreme-loss distributions using the methods of Bayesian inference of the probability of making a claim and Monte Carlo simulation of systemic losses under a possible supply chain. This phase makes sure that premiums are reflectively equivalent in comparison to risk in addition to the establishment of capital needs in the event of tail risks.

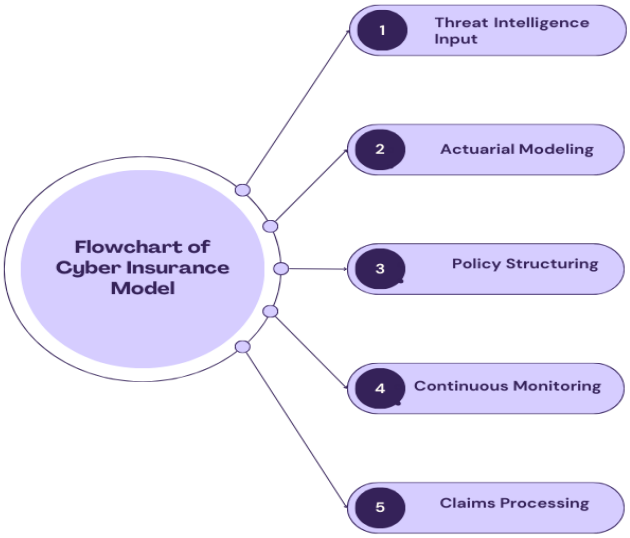

Figure 3. Flowchart of Cyber Insurance Model

- **Policy Structuring:** The product of actuarial modeling is directly incorporated into policy structuring, when coverage limits, deductibles, exclusions, and endorsements are created. As an example, exclusions in relation to state-sponsored attacks on computers or ransomware under special conditions can be instituted to cover uninsurable risks. Meanwhile, by encouraging insured companies to use minimum cybersecurity measures, the premiums may be decreased and the incentives of the insurer and the client aligned.
- **Continuous Monitoring:** Cyber risk is highly dynamic and should be continually monitored even post the underwriting phase. Continuous monitoring involves re-evaluating the exposures according to any new exposure threat intelligence, client security posture measures, and industry-wide incident data. This stage ensures that one can make real-time adjustments to the premiums, or cover and improves the ability of the insurer to anticipate the systemic vulnerabilities until they escalate into a claims situation.
- **Claims Processing:** Finally, once an event has occurred, then the aspect of claims processing would be involved to justify, evaluate and compensate the losses within the provisions of the policy. This encompasses forensic analysis, confirmation of fulfilling the policy conditions and contacting external vendors to heal up. Good claims management is not only helping clients recover but also injecting the lessons learned into the threat intelligence and actuarial modeling processes, which constitute a kind of a feedback mechanism that reinforces the entire insurance process.

3.4. Implementation Considerations

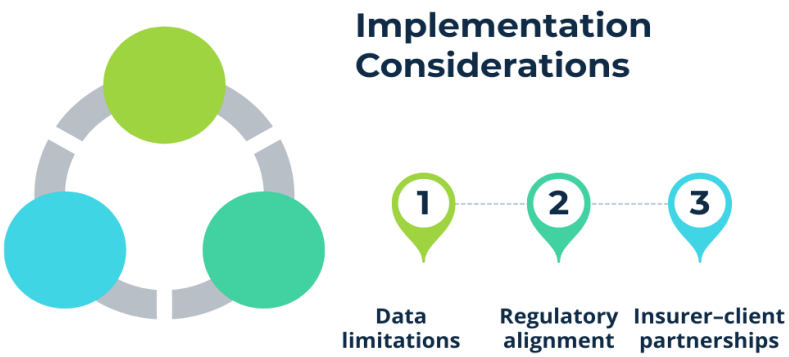

Figure 4. Implementation Considerations

- **Data Limitations:** One of the primary issues of a cyber insurance structure implementation is the scarcity and variety of data. [16-18] Historical breach and ransomware data are often incomplete, disheterogeneously reported, or company specific; difficult to statistically specify and actuarialize. Moreover, reporting infrequently or lack of clarity in regulations lead to the distortion of the loss estimation because of reputational pressures. A good implementation will therefore involve the incorporation of a diversity of data feeds, industry reports and threat intelligence feeds, insurer claim history, and cross sector anonymised datasets, in a bit to make the models and act as a reflector of common and extreme incidents.

- **Regulatory Alignment:** The functions of cybers insurance must be under a complicated regulatory environment, which varies depending on jurisdictions. Under GDPR and EU NIS Directive, among others, policy, claims management and reporting requirements are determined, and state level cybersecurity requirements in the United States are determined. Failure to comply with the ruling conditions may result in fines, court cases on the insurers part and reputational losses. This must be done with proactive compliance policies, standard reporting templates and regular auditing of them in order to ensure that they keep the policies in line with the evolving legal frameworks, the policies, underwriting policies and procedures concerning the response to incidents.
- **Insurer–Client Partnerships:** Mighty cyber insurance designs mandate vigorous relations among the insurers and clients. The insurers can not simply be instructed through prior data and must act with clients to create enhanced security positions, take measures to reduce risks, and make sure they enforce the best patterns. The partnerships enhance risk transparency, reduction in moral hazard and also, a closer fit in actuarial modeling. Secondly, continuous communication would allow insurers to provide dynamically adjusted coverage, precursorial service, and modify policy terms to address the new threat and, in this manner, the benefits between the two parties, a win-win strategy on cyber risk management.

4. Results and Discussion

4.1. Simulation Outcomes

The outcomes of the simulation of the proposed cyber insurance model include quantitative data about the personal danger of ransomware and systematic vulnerability to the supply chain. The model serves to model the process of Bayesian inference when updating probability of ransomware claims according to observed incidents, and obtains probability distributions, the probability of claims in the insured portfolio. It is typical distribution occurring in right skewed with high occurrence of small scale or medium events including occurrence of extreme events on the tail which is in line with the traditions of historical ransomware. Probability density function may be drawn by graphical means to depict that the distribution possesses a peaked value in low-incident directions with a large tail to high-loss directions to represent that the worst but rare may occur. Such visualizations will assist underwriters to reflect on how many claims they will expect to make in the future, what regions of this would be more open to high-risk exposure, and policies that are politically generous and financially viable. Correlated supply chain risk will then be modeled by Monte Carlo simulation in order to define systemic dependencies. The simulation measures the risk of cascading failures potentially involving a number of insureds by drawing repeatedly samples of joint distributions of interdependent firms, cloud providers and critical suppliers.

The outcome of these stress tests reflect the average distinctions in the portfolio under basis, nevertheless, too, the distinctions at the extreme percentiles- pivotal in examining the tail-risks and capital-sufficiency. The results indicate that there are scenarios in which a person or a poorly supplied vulnerability or a underutilized vulnerability has spiked claims and how the aggregate exposure can drive up protective losses greatly exceeding the aggregate impact of the underlying actual probability of incidents. In its operation, these simulations operate strategic resolutions including the structuring of reinsurances, coverage limits, contingency planning, etc. Generally, the ransomware probability distributions and the Monte Carlo systemic stress tests can be applied in providing an overall view of cyber risk with a mix of frequency and correlation of events and in reaction to a network level. The foregoing results show how meaningful dynamic, data-driven actuarial modelling and conducting proactive risk mitigation measures can be so that insurers can be well placed to identify, position, and react to both routine and non-routine cyber-loss events effectively.

4.2. Key Findings

Table 1. Key Findings

Metrics	Improvements
Request Controls	36.5%
Supply Chain Systemic Risk	100%

- **Request Controls (36.5):** In the simulation results provided above, it can be seen that probability of ransomware claims can be reduced by approximately 35 percent in the presence of the obligatory security controls. underscores the importance of foundational cybersecurity controls (i.e. multi-factor authentication, endpoint protection, regularity of patch management and employee awareness training) in reducing risk. This knowledge can be used by the insurers by providing incentives to the insured organizations to put such controls in place by offering them premium discounts, policy-endorsements or conditional coverage. Although 35% drop is significant, it further highlights the importance of supplementary measures that reduce the risk to zero level and the complementary approach is risk transfer mechanisms, i.e. insurance cover and contingency plan.
- **Supply Chain Systemic Risk (100%):** Aggregate exposure is the most important factor that causes extreme losses with the supply chain systemic risk contributing up to 100 percent in the stress cases. As with failures or compromises at critical suppliers or service providers, unlike isolated ransomware events, any failure or compromise by a single supplier or service vendor can ripple throughout multiple insured entities, with simultaneous claims greatly increasing overall portfolio risk. As shown by the simulation, software platform, cloud services, or critical third-party vendors

are highly concentrated to form a single point of failure, so it is not so effective to diversify. The discovery identifies, among others that insurers ought to be able to work out modeling of interdependencies, the stress test of scenarios, design policy or reinsurance schemes, which explicitly incorporate systemic exposures to minimize solvency, when caught in correlated distributions of losses.

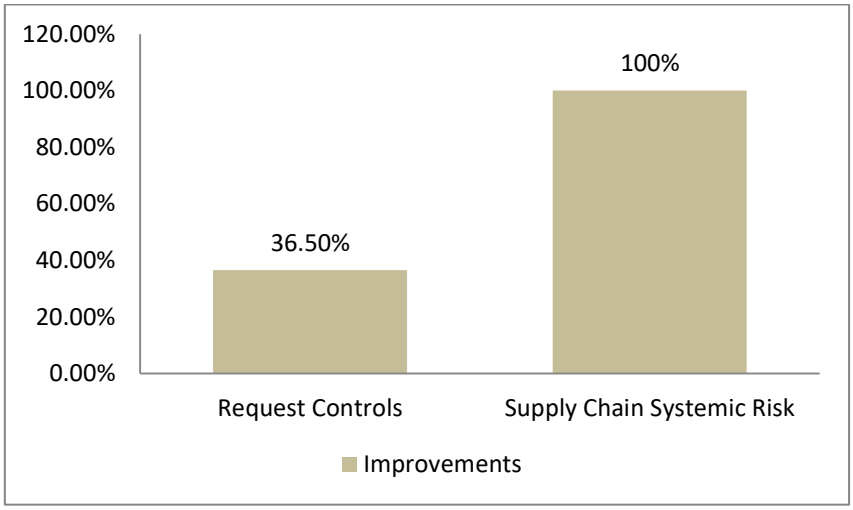

Figure 5. Graph representing Key Findings

4.3. Industry Implications

The transformations in the cyber risk environment that were immediate have triggered certain major alterations in practices and regulatory factors within the industry. The first is that continuous monitoring is becoming a key principle of risk management by the insurers. Traditional underwriting in which a great deal of weight was given to the historical evaluation of historic loss data is not applicable in this swiftly evolving threat context. Real time monitoring helps insurers monitor the stance of client security, threats facing the network and vulnerabilities and provide more dynamic inputs their actuarial model and more responsive pricing can be provided. This proactive approach also contributes to early interventions where clients correct the threats before they turn into claims that eventually reduces the number and scope of losses. The other fact that could be observed is the increase in the policy exclusions and conditional endorsements. As ransomware, failure in supply chains, and other systemic risks continue to gain prominence, policy wording is being constricted in assuring that tail risk is addressed and unwanted accumulations are avoided. Blockage of critical infrastructure, attacks with the support of the state are becoming progressively more frequent, or certain forms of cyber extortion are more common. To the extent that these exclusions limit the insurance in the event of extreme events, they provide incentive to invest in preventive controls against such events and the establishment of robust internal controls.

Actuarial modelling facilitates threat intelligence to support the insurers in the balancing of risk transfer and/or coverage provisions, which will consequently be both commercially feasible and attractive to the clients. Finally, the fiscalizing of cyber insurance markets is emerging as the pillar of sustainable development as the regulatory harmonization needs to take place. Underwriting, risk aggregation and claims management are problematic due to disjointed and inconsistent jurisdictional regulation requirements. As an example, differences in breach notification, liability rules, sanctions compliance may play an important role in losses expected and policy enforceability. Coherent structures, such as EU directives or standard state structures as role models in the U.S., would improve the availability of information, reduce volumes of compliance, and allow uniformity of reporting. Such regulatory consistency, not only increases market stability, but also increases the effectiveness of the management of accumulation and systemic risk assessment. Combined, all these shifts in the industry mix of unremitting monitoring and advanced policy exclusion, and coordination of regulatory efforts, is an indicator of a cyber insuring market coming of age, focusing on proactive risk avoidance, operational stability, and convergence of insurers, users, and regulators around addressing an increasingly complex cyber menace.

5. Conclusion

Cyber insurance has evolved into being not a passive risk transfer device and rather a proactive and strategic part in enterprise cyber risk management. Rise of sophisticated threats particularly ransomware attacks and supply chain attacks has been a dent in otherwise typically customary underwriting habit, how claims are handled and inadequacies of models that rely solely on past loss data. The frequency and extent of modern cyber losses are demonstrated in the presence of Ransomware attacks, which are becoming more frequently delivered by the Ransomware-as-a-Service model, and the interconnectedness of digital infrastructures to vulnerable provider chains such that a single victimized vendor can introduce a cumulative number of disruptions to dozens of insured businesses. These transformations project the necessity of making sure that the insurers adopt

dynamic forward-looking strategies that see them anticipate the forthcoming risks rather than react to those that are being observed.

To both maximize the probability of individual claims and systemic risk of a portfolio, the hybrid structure proposed in this paper by integrating a Bayesian inference process, Monte Carlo simulating, and real-time threat threat intelligence was proposed. Bayesian procedures enable insurers to revise probabilities of ransomware claims on a continuous basis due to the emerged data and threat indicators and provide a rational and statistically valid fashion of the uncertainty model. This is supplemented by Monte Carlo simulation that explores the extreme tail events and correlated losses related to supply chain events, which reveals the potential accumulating risk that would not have been clearly seen otherwise. Threat intelligence will aid in ensuring that the model is updated accordingly to the real trends of the practice of techniques used by attackers, exposures of vulnerabilities and risks unique to the areas. Simulation outcomes illustrate the application of such a hybrid model in the measurement of the impact of the necessary security controls, systemic exposures, and guide pricing and capital allocation decisions.

The industry is interested in the results. Underwriting and risk management is increasingly becoming a part of real-time surveillance wherein the insurer can dynamically adjust the coverage, its premiums and mitigation incentives. Policy exclusion and conditional endorsements to address tail risk and regulatory convergence across jurisdictions are becoming important in the promotion of uniformity in reporting breaches, legal compliance and risk assessment. These strategies combined help facilitate cyber insurance as a source of financial protection, a proactive method to cybersecurity, and resiliency. In the future, it is possible to discuss the application of AI-based round-the-clock surveillance with the ability to provide predictive value, automated threat detection, and application optimization to the automatic process of adjusting premiums dynamically. Moreover, the blockchain-based smart contracts may enable the opportunity to verify the claims and resolve them automatically with the highest level of transparency, which can reduce the number of disputes and administrative delays. Coupled with these technologies, cyber insurance once again can become a real time, living risk management platform, able to produce synergies between the interests of the insurers and the clients, and stay financially viable against the more complex and interconnected cyber threats.

References

[1] Böhme, R., & Schwartz, G. (2010, June). Modeling cyber-insurance: towards a unifying framework. In WEIS.

[2] Karri, N. (2021). Self-Driving Databases. International Journal of Emerging Trends in Computer Science and Information Technology, 2(1), 74-83. https://doi.org/10.63282/3050-9246.IJETCSIT-V2I1P10

[3] Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance-Issues and Practice, 40(1), 131-158.

[4] Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121-135.

[5] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015, June). Cutting the gordian knot: A look under the hood of ransomware attacks. In International conference on detection of intrusions and malware, and vulnerability assessment (pp. 3-24). Cham: Springer International Publishing.

[6] Karri, N., Pedda Muntala, P. S. R., & Jangam, S. K. (2025). Predictive Performance Tuning. International Journal of Emerging Research in Engineering and Technology, 2(1), 67-76. https://doi.org/10.63282/3050-922X.IJERET-V2I1P108

[7] Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J. W., & Winkelman, Z. (2018). Estimating the global cost of cyber risk. Research Reports RR-2299-WFHF, Rand Corporation.

[8] Regulation, P. (2018). General data protection regulation. Intouch, 25, 1-5.

[9] Karri, N. (2022). AI-Powered Anomaly Detection. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 3(2), 122-131. https://doi.org/10.63282/3050-9262.IJAIDSML-V3I2P114

[10] Enjam, G. R. (2020). Ransomware Resilience and Recovery Planning for Insurance Infrastructure. International Journal of AI, BigData, Computational and Management Studies, 1(4), 29-37.

[11] Kshetri, N. (2020). The evolution of cyber-insurance industry and market: An institutional analysis. Telecommunications policy, 44(8), 102007.

[12] Kurmaiev, P., Seliverstova, L., Bondarenko, O., & Husarevych, N. (2020). Cyber insurance: the current situation and prospects of development. Amazonia Investiga, 9(28), 65-73.

[13] Karri, N., Pedda Muntala, P. S. R., & Jangam, S. K. (2022). Forecasting Hardware Failures or Resource Bottlenecks Before They Occur. International Journal of Emerging Research in Engineering and Technology, 3(2), 99-109. https://doi.org/10.63282/3050-922X.IJERET-V3I2P111

[14] Camillo, M. (2017). Cyber risk and the changing role of insurance. Journal of Cyber Policy, 2(1), 53-63.

[15] Robinson, A., Corcoran, C., & Waldo, J. (2022). New risks in ransomware: Supply chain attacks and cryptocurrency.

[16] Kenneally, E. (2021). Ransomware: a Darwinian opportunity for cyber insurance. Conn. Ins. LJ, 28, 165.

[17] Chockalingam, S., Pieters, W., Teixeira, A., & van Gelder, P. (2017, November). Bayesian network models in cyber security: a systematic review. In Nordic conference on secure IT systems (pp. 105-122). Cham: Springer International Publishing.

[18] Sommer, P., & Brown, I. (2011). Reducing systemic cybersecurity risk. Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS (2011), 3.

[19] Karri, N. (2022). Predictive Maintenance for Database Systems. International Journal of Emerging Research in Engineering and Technology, 3(1), 105-115. https://doi.org/10.63282/3050-922X.IJERET-V3I1P111