risks

MDPI

Article

An Analytical Review of Cyber Risk Management by Insurance Companies: A Mathematical Perspective

Maria Carannante [1] **and Alessandro Mazzoccoli** [2,*]

[1] Department of Human Science, European University of Rome, Via degli Aldobrandeschi 190, 00163 Rome, Italy; maria.carannante@unier.it
[2] Department of Economics, Roma Tre University, Via Silvio D'Amico 77, 00146 Rome, Italy
* Correspondence: alessandro.mazzoccoli@uniroma3.it

Abstract

This article provides an overview of the current state-of-the-art in cyber risk and cyber risk management, focusing on the mathematical models that have been created to help with risk quantification and insurance pricing. We discuss the main ways that cyber risk is measured, starting with vulnerability functions that show how systems react to threats and going all the way up to more complex stochastic and dynamic models that show how cyber attacks change over time. Next, we examine cyber insurance, including the structure and main features of the cyber insurance market, as well as the growing role of cyber reinsurance in strategies for transferring risk. Finally, we review the mathematical models that have been proposed in the literature for setting the prices of cyber insurance premiums and structuring reinsurance contracts, analysing their advantages, limitations, and potential applications for more effective risk management. The aim of this article is to provide researchers and professionals with a clear picture of the main quantitative tools available and to point out areas that need further research by summarising these contributions.

Keywords: cyber insurance; cyber risks; mathematical models; pricing

check for updates

Academic Editor: Andrea Consiglio

Received: 9 July 2025
Revised: 24 July 2025
Accepted: 29 July 2025
Published: 31 July 2025

Citation: Carannante, Maria, and Alessandro Mazzoccoli. 2025. An Analytical Review of Cyber Risk Management by Insurance Companies: A Mathematical Perspective. *Risks* 13: 144. https://doi.org/10.3390/risks13080144

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Cyber risk is characterised by a combination of factors that complicate its measurement, management, and transfer (Aven et al. 2018; Eling et al. 2021; Zeller and Scherer 2022). First, the lack of reliable historical data (Zängerle and Schiereck 2023), exacerbated by companies' reluctance to disclose incidents for fear of reputational damage, makes it difficult to build robust loss models. Second, cyber risk is inherently dynamic: it evolves alongside technological innovation, regulatory developments, and the increasing speed and scope of digital transformation, continuously creating new vulnerabilities (Georgescu 2021; Smith and Lostri 2020). In particular, Ratnawat (2025) focused on how AI can benefit small- and medium-sized businesses in the use of cyber insurance from an insurtech perspective. Mupa et al. (2025) reinforced this point, demonstrating an AI-based approach to assessing operational risk for insurance companies and pricing cyber policies. On the other hand, Zraqou et al. (2025) highlighted the rise in AI-risks, linked to the use of insurtech tools. Furthermore, Novo et al. (2025) proposed a review of emerging cyber risks due to the development of smart cities. Actually, Wheatley et al. (2016) and Xu et al. (2018) observed a growing number of significant incidents and higher frequency attacks. Also, Palsson et al. (2020) and Pollmeier et al. (2023) confirmed an increasing trend in cyber incidents. Third, unlike many traditional risks, cyber incidents are often intentional acts carried

out by strategic threat actors driven by economic or political reasons, supported by a mature cybercrime ecosystem offering tools and services on demand (Abou El Houda 2024; Munk 2022). Furthermore, the high degree of interconnectivity between IT systems creates interdependence and accumulation risks, where a single vulnerability can have cascading effects across networks and sectors (Kröger 2008; Maglaras et al. 2018). This interconnectedness also generates negative externalities, as underinvestment in security by one entity can weaken the overall resilience of the network. Adding to this complexity is the challenge of quantifying the economic impact of intangible information assets and managing information asymmetries, such as adverse selection and moral hazard, which hinder effective cyber insurance solutions (Franke 2017). In this sense, Pal et al. (2025) proposed a framework relating to the information asymmetry linked to chain propagation along the supply chain of a cyber attack, and the need for the insurance company to obtain information relating to the interdependence of the insured portfolio. These issues have also led to an increasing body of literature on how to manage cybersecurity (e.g., Ghelani 2022; Lallie et al. 2021; Taherdoost 2022; Venkatachary et al. 2017). Furthermore, Allianz Commercial (2025) states that cyber risk is the one that worries companies the most, consolidating its position compared to previous years. The main causes lie in the interdependence of risks with other issues and the increase in attacks due to the improvement in AI and related technologies. The issue of security is not only about technology, but also about the possibility of hedging losses through adequate instruments. In this context, insurance companies play a fundamental role. Significant cyber-related risks have arisen in the insurance industry as a result of the growing digitalisation of financial services. According to European Insurance and Occupational Pensions Authority (2023), insurers' vulnerability to cyber threats is twofold: they are exposed to breaches as IT users, and, on the other hand, they are indirectly exposed due to underwriting risk from cyber insurance products. Cyber attacks can limit the operational activities of insurers to fulfil contractual obligations and guarantee their continuity, with consequent risks to policyholders and broader financial stability. For this reason, insurance companies are required to integrate the ability to withstand, respond to, and recover from cyber incidents into supervisory stress test exercises, to quantify the financial impact of adverse cyber scenarios, and to assess the adequacy of risk management practices. At the same time, the expansion of the cyber insurance market reflects a greater awareness of digital vulnerabilities among companies and individuals, which inevitably exposes insurance companies to a greater underwriting risk. To these, the issue of non-affirmative cyber risk is added, which occurs when traditional insurance products inadvertently provide coverage for cyber events. These exposures are often not recognised in the underwriting processes, leading to potential misalignments between the risk and premium. With the increase in the frequency and severity of cyber events, the inability to accurately outline and assess these risks can lead to unexpected loss accumulations and greater volatility in insurers' claims experience. An additional area of concern is the risk of cyber accumulation, where a widespread ransomware attack or a significant disruption at a commonly used cloud service provider can impact a substantial portion of an insurer's portfolio. The interconnection of cyber risk is a key point to manage, and it requires specific modelling to be included in the stress test. In other words, the stress-testing methodologies related to cyber risk must consider both their role as targets of cyber attacks and as facilitators, ensuring not only that they can recover internally from cyber incidents but also that they are resilient to potential accumulation losses arising from their underwriting activities to safeguard the stability and reliability of the insurance sector integrated into the IT system. The increasing exposure to cyber risk has led to the exploration, quantification, and classification of the phenomenon. In this context, Lopez et al. (2025) proposed an integrated framework for risk

quantification, stress scenario construction, and insurance solution design, highlighting the inherent complexity of modelling dynamic and interconnected risks. On the other hand, Rabitti et al. (2025) highlighted the excess of taxonomies about the cyber risk, which could lead to confusion, and proposed a comparative review of the main cyber risk taxonomies, highlighting significant divergences in classification criteria and emphasising the need for standardisation to improve interoperability and consistency in assessments.

This aspect is certainly important for a correct assessment of the problem and for choices in terms of both security and design of insurance products. In this sense, Strzelczyk and Puławska (2025) explored how insurance can not only cover financial losses but also incentivise virtuous behaviour in terms of cybersecurity investments. A similar result was stated by Adriko and Nurse (2024), showing how information gathering by insurance companies helps define best practices, even though the market is significantly undersized compared to the risk. However, the effectiveness of this mechanism largely depends on insurers' ability to correctly assess the risk profile of policyholders. In this regard, Rangu et al. (2024) analysed the critical issues and gaps in the risk analysis frameworks adopted by insurance companies, highlighting how the lack of standardised metrics and structured data represents an obstacle to market efficiency.

The aim of our review is to investigate the mathematical tools available for insurance companies to manage several issues related to cybersecurity. In particular, this paper analyses the quantitative aspects of the regulatory framework to determine the fair premium and the capital requirements, the model devoted to claims evaluation and insurance pricing, and some financial instruments for reinsurance. The paper is structured as follows. Section 2 provides an overview of the state-of-the-art on cyber risk and cyber risk insurance. This is followed by Section 3, in which the quantification of cyber risk history is presented. Section 4 is devoted to cyber insurance quantification, focusing on the interdependence issue. Section 5 examines the main mathematical models for insurance pricing. Finally, Section 6 concludes the article.

2. Overview of the State-of-the-Art

This section aims to provide an overview of the current state of academic and industry research on cyber risk and cyber insurance. It examines how scholars have approached the modelling, prediction, and management of cyber threats, highlights the unique features that distinguish cyber risks from traditional insurable risks, and summarises the main challenges that still hinder the development of mature insurance solutions. By reviewing key contributions in the field, this section identifies existing knowledge gaps and emerging research directions, offering a foundation for future work on more robust and effective risk transfer mechanisms. The first contribution in this field is given by Marotta et al. (2017), providing a comprehensive overview of the state of knowledge on cyber insurance, combining perspectives from both the market and academia. Their survey defines key concepts and clarifies the formal foundations of cyber insurance as a distinct line of business within the insurance industry. They examine the main features that differentiate cyber insurance from conventional products, such as the intangible nature of the insured assets, the evolving threat landscape, the potential for large-scale correlated losses, and the role of risk accumulation through interconnectivity. The paper discusses how technological factors—including the adoption of digital infrastructures, cloud computing, and IoT devices—create new risk vectors and complicate risk assessment and underwriting processes. Moreover, Marotta et al. (2017) compared various scientific approaches to analysing the cyber insurance market, ranging from theoretical models of market equilibrium and adverse selection to empirical studies of market penetration, product design, and claims data. This synthesis helps establish a shared foundation for researchers and practitioners

to build upon. Moreover, Carfora et al. (2019) contributed an actuarial perspective on cyber risk management, highlighting how traditional actuarial methods can be adapted to the context of cyber threats. Their paper focuses on the development and application of actuarial models for quantifying and pricing cyber risk, emphasising the need to account for the high degree of uncertainty and the interdependent nature of cyber events. They also discuss challenges in defining appropriate risk measures, collecting reliable data, and integrating dynamic threat intelligence into actuarial frameworks. By bringing an actuarial lens to cyber risk, their work bridges the gap between cybersecurity practice and quantitative risk modelling, underscoring the potential for actuarial science to support more robust and resilient cyber insurance solutions. Eling (2020) presented one of the most influential and structured reviews on cyber risk and cyber insurance, focusing on how these topics are addressed within the disciplines of management, economics, finance, risk management and insurance, and actuarial science. Their study shows that, although the relevance of cyber risk has grown substantially in recent years, it remains under-explored in business and actuarial research compared to its practical impact on organisations and markets. Specifically, business studies have primarily examined the adverse effects of cyber incidents through event studies and scenario-based analyses, revealing how cyber attacks influence stock prices, firm value, and operational continuity. Meanwhile, economic research emphasises the trade-offs involved in cyber risk management decisions, exploring how firms balance investments in prevention, detection, and transfer of risk through insurance. In the actuarial domain, quantitative models tend to focus on loss modelling, often investigating the statistical properties of cyber incidents, including frequency, severity, and interdependence. Notably, Eling (2020) categorised the empirical contributions in terms of how they address the dependencies between cyber risks, highlighting the role of network structures and contagion effects that make cyber risks fundamentally different from traditional insurable risks. This categorisation provides a clearer understanding of what is currently known about the distributional characteristics and correlation structures of cyber incidents, while also pointing out critical gaps in the empirical evidence base. Dubois et al. (2022) analyses the state of the art in cyber risk modelling both from academic literature and "grey" sources to provide actuaries with guidance on both the most used quantitative approaches and the available data sources, underlining the need for greater collaboration between different disciplines, the development of shared datasets, and the adoption of empirically validated models. The report highlights that while there is a great interest among computer scientists, actuaries are still little involved in analysing cyber risk. In this line of research, Cremer et al. (2022) expanded this perspective by critically analysing both academic and industry literature with a specific focus on the availability, quality, and limitations of cyber risk data. Their review underscores that one of the major barriers to advancing research and practical risk modelling in this field is the scarcity of reliable, standardised, and publicly accessible data on cyber incidents. The authors discuss how data gaps affect the accuracy of risk assessment, hinder the development of robust actuarial models, and limit the effectiveness of insurance products. They also identify emerging trends in data-sharing initiatives, regulatory reporting requirements, and collaborative efforts among insurers and firms aimed at improving the transparency and consistency of cyber risk information. In their comprehensive survey, Awiszus et al. (2023) examined the complexity of cyber risk modelling and insurance pricing frameworks, proposing a three-fold taxonomy of cyber risks: idiosyncratic, systematic, and systemic, each with distinct characteristics and modelling implications. In particular, idiosyncratic risks, arising from isolated incidents such as internal errors or targeted attacks on individual firms, are assumed to be independent across entities. These are well-suited to traditional actuarial techniques, leveraging frequency–severity models and classical premium principles

to assess claim distributions. Systematic risks relate to common vulnerabilities shared across exposures, leading to correlated loss events, and can be modelled via common risk factors as in the classical frameworks. Finally, systemic risks represent the most difficult to model category, involving contagion mechanisms, showing non-linear dependencies and requiring advanced modelling strategies such as epidemic network models or game-theoretic systems to capture infection dynamics and behavioural interactions. Additionally, Dacorogna and Kratz (2023) provided a valuable perspective by framing cyber risk as a key component of modern operational risk. They discuss how traditional actuarial and quantitative models—originally designed for well-understood risks with stable statistical properties—must evolve to address the unique features of cyber threats, such as heavy-tailed loss distributions, contagion effects, and high uncertainty. The survey detects three layers of cyber risk: hardware, software, and psycho-cognitive, highlighting the importance of combining empirical data with expert judgement to quantify low-frequency, high-severity events like cyber incidents. Furthermore, Tsohou et al. (2023) added to this body of work by providing an extensive review of the literature on cybersecurity insurance, spanning both research and practice. They outline the evolution of the field, describe the current state of the market, and identify emerging trends and open issues. Among these are the increasing need for more tailored insurance products, the development of standardised policy terms, and the role of policy and regulation in shaping coverage and market growth. Their synthesis underscores the importance of interdisciplinary research and collaboration between academia and industry to tackle the complex challenges of insuring cyber risks. Adriko and Nurse (2024) analysed the relationship between cybersecurity, cyber insurance, and small- and medium-sized enterprises. The study arises from the growing awareness that small- and medium-sized enterprises are increasingly exposed to cyber threats, but often lack the resources, knowledge, and adequate tools to effectively address them. In this context, cyber insurance is proposed as a possible financial and technical support. On the one hand, cyber insurance can offer concrete value to small- and medium-sized enterprises, providing financial protection in the event of incidents, access to specialised services, and incentivising the adoption of good security practices. On the other hand, several barriers to adoption emerge, such as the difficulty of companies in understanding and assessing their cyber risks, the complexity of insurance policies available on the market, and the lack of internal technical skills. The need to develop clearer and more standardised tools to help small- and medium-sized enterprises in assessing cyber risk is also highlighted. Overall, the article represents an original and significant contribution, as it is one of the first studies to offer a comprehensive and critical view of the intersection between cyber insurance and cybersecurity in the context of small- and medium-sized enterprises, highlighting both the potential of this combination and the current limitations that hinder its full effectiveness. Finally, He et al. (2024) offered a more recent and cross-disciplinary perspective, providing a structured review of the literature on cyber risk modelling and insurance to bridge the gap between computer engineering, actuarial science, and business studies. Their work highlights the evolution of methodologies used to predict and model cyber risks, including stochastic models, simulation-based approaches, machine learning techniques, and scenario analysis. They also emphasise the importance of integrating technical insights from computer science, such as vulnerability analysis, threat intelligence, and network topology, into actuarial and insurance models to better capture the dynamic and interconnected nature of cyber risks. By categorising the existing contributions according to their modelling frameworks and underlying assumptions, the authors help identify promising avenues for future research, including hybrid models that combine statistical and engineering-based approaches to improve prediction and pricing accuracy.

3. Brief History of Cyber Risk Quantification

The development of early models for cyber risk analysis will be briefly reviewed in this section, with an emphasis on the major advancements and the introduction of more sophisticated techniques. In order to comprehend the nature and variability of cyber threats, we will also look into different risk distribution descriptions. The first two theoretical models aimed at assessing the cybersecurity vulnerability of an organisation were proposed by Gordon and Loeb. A key element of the model introduced in their seminal paper Gordon and Loeb (2002) is the vulnerability function, which expresses the probability that information is compromised as a function of the level of investment in security measures. This function is fundamental because it allows modelling the protective effect of investments: as spending on information protection increases, the probability of a successful attack decreases, although with diminishing marginal returns. The vulnerability function $v : \mathbb{R} \to [0, 1]$ is typically defined as decreasing and concave, reflecting the intuition that each additional unit of investment i in security provides progressively smaller benefits in terms of risk reduction. This structure enables a rational evaluation of the trade-off between protection costs and the value of information at risk, helping to avoid both underinvestment, which exposes the organisation to significant damage, and overinvestment, which is inefficient and wasteful. The two vulnerability models are described by the following functions:

$$v = \frac{v_0}{(\alpha i + 1)^{\beta}} \tag{1}$$

$$v = v_0^{\alpha i + 1} \tag{2}$$

where v_0 represents the vulnerability in the absence of any security investment, and α and β are parameters that modulate the effectiveness of the security investment i. While the first is linear in the vulnerability variable in the absence of investment (v_0), the second is non-linear with respect to v_0, providing a more sensitive and refined model for describing overall vulnerability. The importance of this model lies in its ability to integrate cybersecurity risk into an economic framework, offering an operational criterion for determining the optimal level of investment in security (see also Gordon et al. 2014, 2016, 2020). The most well-known and cited result from the model is that it is never economically rational to invest more than 37% of the expected loss value to protect information. This limit provides a useful guideline, especially in contexts where vulnerability is significant but available resources are limited. Further models following Gordon and Loeb's work were introduced by Hausken (2006). In particular, he proposed four models for describing the vulnerability of a firm, the last three of which can be grouped under a single function, though they differ in how vulnerability is modelled based on parameter ranges. The first model introduced by Hausken (2006) takes the following form:

$$v = \frac{v_0}{1 + \alpha(e^{\beta i} - 1)} \tag{3}$$

where the parameters measure the effectiveness of security investments. The peculiarity of this model lies in the fact that there exists an intermediate level of investment at which the curve describing a firm's vulnerability changes concavity (from concave to convex). The remaining three models can be summarised under a single function:

$$v = \begin{cases} v_0(1 - \alpha i^{\beta}) & \text{if} \quad i \leq \alpha^{-1/\beta} \\ 0 & \text{if} \quad i > \alpha^{-1/\beta} \end{cases}. \tag{4}$$

In all three models, the parameter $\alpha > 0$, while they differ in the range of values that β can take. In the first of the three, $\beta \in (0,1)$; in the second, $\beta > 1$; and in the third, $\beta = 1$.

Three additional models were introduced by Wang (2017), namely the Exponential Power Model, the Proportional Hazard Model, and the Wang Transform.

$$v = v_0 \alpha^{i^{\beta}} \tag{5}$$

$$v = v_0 (1 - \alpha^{i^{-\beta}}) \tag{6}$$

$$v = v_0 G(G^{-1}(\alpha) - \beta \ln(i)) \tag{7}$$

where $G(\cdot)$ is the cumulative distribution function of the standard normal distribution. In all three models, $\beta > 0$ and $\alpha \in (0,1)$. In fact, in these models, Wang assumes $v_0 = 1$, thus implying that a system is fully vulnerable in the absence of security investments ($i = 0$). Equations (5)–(7) represent a generalisation of the functions introduced by Wang.

The vulnerability functions are summarised in Table 1.

Table 1. Summary of the vulnerability functions and their mathematical formulations. v_0 is the vulnerability when no investment was made, i is the investment in security, and α and β are two positive parameters that describe the effectiveness of the investment on the vulnerability.

Vulnerability Function	Mathematical Formulation
Function 1	$v = \frac{v_0}{(\alpha i+1)^{\beta}}$
Function 2	$v = v_0^{\alpha i+1}$
Function 3	$v = \frac{v_0}{1+\alpha(e^{\beta i}-1)}$
Function 4–6	$v = \begin{cases} v_0(1-\alpha i^{\beta}) & \text{if } i \leq \alpha^{-1/\beta} \\ 0 & \text{if } i > \alpha^{-1/\beta} \end{cases}$, $\beta \in (0,1)$ or $\beta = 1$ or $\beta > 1$
Function 7	$v = v_0 \alpha^{i^{\beta}}$
Function 8	$v = v_0 (1 - \alpha^{i^{-\beta}})$
Function 9	$v = v_0 G(G^{-1}(\alpha) - \beta \ln(i))$

The Gordon and Loeb model has been extended and refined in various ways to better capture the complexities of real-world cybersecurity investment decisions. For example, Kuper et al. (2020) examined under what conditions it is economically rational to invest in cybersecurity, highlighting the existence of a critical threshold of vulnerability where such investments become worthwhile. Building on this, Mazzoccoli and Naldi (2021) developed a dynamic extension of the Gordon–Loeb framework, accounting for asset depreciation and time-dependent returns, and suggesting that optimal investments should adapt over time. Young et al. (2016) contributed a flexible decision-making framework that incorporates uncertainty about cyber risks, allowing organisations to adapt their security strategies as new information emerges. Meanwhile, Matsuura (2008) linked cybersecurity investments directly to productivity gains, emphasising that better security can also enhance overall business performance. Skeoch (2022) expanded the traditional Gordon–Loeb approach by introducing systemic risks, showing how interconnections between organisations can lead to cascading effects that increase the optimal level of investment. In a similar vein, Mazzoccoli and Naldi (2022b) optimised cybersecurity spending by jointly considering insurance solutions and complex market dynamics, illustrating how security and insurance can be combined for better risk management. Wang (2019) proposed an integrated cost–benefit model for cybersecurity that goes beyond the original static framework, weighing security spending against insurance premiums and expert costs. Krutilla et al. (2021)

also extended the analysis to a dynamic, multi-period setting, evaluating how the benefits of cybersecurity investments evolve over time and contribute to broader public welfare. Focusing on inter-organisational dependencies, Gao et al. (2015) incorporated network effects into the investment decision, analysing how firms' security choices influence each other. Huang and Behara (2013) revisits the economics of vulnerabilities with a variant which applies to targeted attacks on specific nodes rather than general threats. Mayadunne and Park (2016) used this simplified Gordon and Loeb version to support risk management decisions for small- and medium-sized enterprises, applying expected utility theory to tailor investment levels. Taking the strategic dimension further, Xu et al. (2019) modelled cybersecurity investments in interactive, multi-actor contexts, introducing game-theoretic elements absent from the original Gordon–Loeb model. All these extensions have been studied and summarised in depth by Mazzoccoli and Naldi (2022a), who provided an extensive review of how the Gordon–Loeb framework has evolved to incorporate dynamics, network effects, insurance integration, and real-world empirical adjustments. Callegaro et al. (2025) presented a stochastic and dynamic version of the Gordon–Loeb model for optimal cybersecurity investment by using a Hawkes process to incorporate temporally clustered cyber attacks. Finally, Franke and Orlando (2025) extended the Wang model to highlight the role of the insurer to stimulate joint investment in cybersecurity to reduce systematic risks and improve the entire business supply chains. Furthermore, several studies focused on the frequency–severity approach to model cyber attacks. In particular, severity follows heavy-tailed distributions (Dacorogna et al. 2023; Dunne and Malone 2017; Eling et al. 2024; Farkas et al. 2021; Strupczewski 2019), while Sun et al. (2021) focused on random variables to model frequency distribution instead of severity, proposing a hurdle Poisson random variable to manage zero attacks on firms and an irregular distribution of breaches. This distribution is combined with a heavy-tailed distribution for severity, taking into account the relationship between frequency and severity, which is generally neglected. An important article regarding the frequency–severity approach is given by Maillart and Sornette (2010). The two authors analysed a dataset of real-world cyber incidents collected between 2000 and 2008, including economic losses caused by attacks such as viruses, hacking, data breaches, and similar events. In particular, they show that the economic damages resulting from cyber incidents follow a heavy-tailed distribution, specifically a power-law distribution:

$$\mathbb{P}(X > x) \sim x^{-\alpha}, \quad x \geq x_{\min}$$

where α is the power-law exponent, and $x_{\min}$ is the threshold above which the distribution effectively follows the power-law behaviour.

The authors estimate α from the observed data in the following way:

$$\hat{\alpha} = 1 + n \left[\sum_{i=1}^{n} \ln \left(\frac{x_i}{x_{\min}} \right) \right]^{-1}$$

where n is the number of observations such that $x_i \geq x_{\min}$.

The empirical value they find is $\alpha \approx 1.7$, which implies a theoretically infinite variance and a highly unstable mean.

This means that while most incidents cause relatively small damages, a small fraction of extreme events can lead to massive economic losses. Traditional risk assessment methods (based on means and standard deviations) are inadequate for modelling cyber risks.

Companies and governments must adopt risk management strategies that account for the possibility of rare but catastrophic events.

Peters et al. (2017) employed clustering and predictive modelling techniques to analyse cyber incident data. For unsupervised classification, K-means clustering is utilised to partition the data by minimising the within-cluster sum of squares:

$$\min_{C_1,\ldots,C_k} \sum_{j=1}^{k} \sum_{x_i \in C_j} \|x_i - \mu_j\|^2,$$

where μ_j denotes the centroid of cluster C_j. Additionally, hierarchical clustering methods are applied to capture the relational structure between clusters based on inter-group distance metrics. Supervised learning approaches are adopted to model incident severity and the likelihood of specific attack types. In particular, logistic regression is used to estimate the probability of a successful cyber attack. To characterise the distribution of cyber losses, parametric models such as log-normal, gamma, and Pareto distributions are employed. Moreover, kernel density estimation is used as a non-parametric technique to obtain smoothed approximations of loss distributions. In the paper by Sobchuk et al. (2023), cyber attacks were represented by a piecewise continuous function $f(t)$, constructed from empirical data (e.g., the number of attacks within specific time intervals). The function $f(t)$ was expanded into a Fourier series as follows:

$$f(t) = a_0 + \sum_{n=1}^{\infty} \left(a_n \cos\left(\frac{2\pi n t}{T}\right) + b_n \sin\left(\frac{2\pi n t}{T}\right) \right)$$

where T is the period of the function (e.g., a fixed time window), and a_n and b_n are the Fourier coefficients, calculated based on the observed data. Weisman et al. (2025) proposed mathematical models to quantify the cyber resilience of the system under study. Let $X(t)$ represent the system performance or state of functionality at time t, where $X(t)$ decreases due to the impact of cyber attacks and recovers over time due to inherent physical resilience and cyber-defence mechanisms. The dynamics of $X(t)$ can be modelled by differential equations of the form

$$dX(t) = -\alpha_1 A(t) X(t) dt + \alpha_2 R(t)(1 - X(t)) dt,$$

where $A(t)$ is the attack intensity function representing the severity or presence of malware attacks at time t, $R(t)$ represents recovery efforts or inherent resilience factors active at time t, and α_1 and α_2 are positive parameters quantifying the effectiveness of attack impact and recovery mechanisms, respectively. This formulation captures the degradation of system performance under attack and its restoration through resilience. The model parameters can be estimated from experimental data obtained during systematic testing of the cyber–physical system. Key quantitative metrics derived from this model include the resilience level, which is defined as the minimum performance level reached during an attack, the recovery time required for $X(t)$ to return to a specified threshold close to full functionality, and the robustness, which quantifies the system's resistance to performance degradation. In particular, these models provide a tractable and interpretable framework for assessing cyber resilience and guiding the design of improved defence strategies. The importance of severity–frequency models relies on their use by insurance to determine the value of the portfolio and the solvency capital requirement. The next section focuses on the insurance market and the issues facing portfolio management and the modelling of tailored cyber risk hedging products.

4. Cyber Insurance

4.1. Managing Interdependence in Insurance Regulation

The insurance market for cyber risk hedging has been expanding in recent years, and this growth has also impacted the regulation and operational risks associated with the products offered by insurance companies. In particular, the European Insurance and Occupational Pensions Authority (EIOPA) investigates cyber risk hedging needs, both on the supply and demand side. European Insurance and Occupational Pensions Authority (2018) satisfies the need to investigate the cyber risk insurance market, understand its dimension, and evaluate the critical issues to be explored in depth. To fill the knowledge gap, a qualitative survey is carried out in 13 European insurance groups to define a general framework of the phenomenon. From the survey, an embryonic phase emerges, with extensive use of qualitative methods for the estimation of pricing, risk exposures, and risk accumulations. Lack of claims data is the most important limitation in properly estimating and pricing risk. In addition, the importance of quantifying non-affirmative risks and operational risks for insurance companies arises. European Insurance and Occupational Pensions Authority (2019) explores the latter aspects, with a quantitative survey of 41 insurance groups, representing approximately three-quarters of the European market. The study shows significant variability in the definition of Solvency Capital Requirements (SCRs) for cyber risk, with significantly different capital requirements; alternatively, some insurers refer to the Solvency II Standard Formula and do not quantify cyber risk directly. EIOPA investigations show the importance of a common regulatory framework and definitions to improve operational resilience and enable more effective dialogue between insurance companies, regulators and authorities, and the need for harmonised claims reporting systems, to enable a more complete and shared view of risk. The opportunity to leverage cyber insurance to increase awareness of digital risk and promote the dissemination of best practices. Alongside these aspects, the need to develop specific quantitative methods to manage non-affirmative exposures emerged, since they are still poorly understood and structured in the market.

At the end of the investigation and discussions with insurance companies and actuaries, European Insurance and Occupational Pensions Authority (2023) defines a regulatory framework to assess insurer resilience under the likely scenarios of cyber adverse events, providing guidelines in terms of events to stress test, metrics to use for assessment, and types of risk to consider, in line with the indications of the Digital Operational Resilience Act (DORA). In particular, EIOPA focused on two main issues: cyber resilience, that is, the ability of an insurance company to withstand the financial impact of an adverse cyber event, and the cyber underwriting risk, that is, the insurance capacity to deal with the capital requirements affecting the insurance hedging, such as liability portfolios. Distinguishing between affirmative and non-affirmative risks, EIOPA indicates the suitable insurance product to define a cyber liabilities portfolio, the size of the financial exposure, in terms of line of business, and the evaluation metrics to adequately perform a stress test. Also in this report, awareness promotion versus the need to perform a stress test on non-affirmative cyber risk emerges. Let N be the number of adverse cyber events and L_i be the associated losses. We define the random variable of exposure risk X as

$$X = \sum_{i=1}^{N} L_i.$$

Assuming L_i are i.i.d. with a generic random variable $\mathcal{L}$, we define the actuarial present value of the insurance contract, that is, the expected value of the risk exposure random variable X as

$$\mathbb{E}[X] = \mathbb{E}[N]\mathbb{E}[L] \qquad \mathbb{V}[X] = (\mathbb{E}^2[L] + \mathbb{V}[L])\mathbb{E}[N], \tag{8}$$

and the distribution of risk exposure is defined as

$$F_X(\ell) = \sum_{i=0}^{\infty} P_n \cdot F_L^n(x)$$

where P_n is the frequency distribution and $F_L^n(x)$ represents the n times convolution of the severity distribution.

Solvency II states the calculation of the Solvency Capital Requirement (SCR) according to two approaches European Commission (2015); European Insurance and Occupational Pensions Authority (2014): the standard formula and the internal model. The former is equal to the sum of the basic SCR ($bSCR$), the capital requirement for operational risks (SCR_{op}), and the adjustment (Adj)

$$SCR = bSCR - Adj + SCR_{op}.$$

Let SCR be the vector of the capital requirement for each risk category SCR_i, it can be defined as

$$SCR = \sqrt{SCR^T \cdot \Sigma \cdot SCR}$$

where Σ is the correlation matrix between different risk categories. The standard formula takes into consideration only linear relationships between predetermined risk categories, whose coefficients are provided by EIOPA. The SCR can also be defined as the gap between the α% Value-at-Risk (VaR) and the actuarial present value of the exposure to risk random variable X:

$$SCR = [VaR_{\alpha\%}(X) - \mathbb{E}[X]].$$

This implies that the SCR can be defined as

$$VaR_{\alpha\%}(X) - \mathbb{E}[X] = \kappa \cdot \sqrt{\Sigma}$$

where κ is the standard deviation factor of a distribution, and VaR is defined as follows:

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

The actuarial present value $\mathbb{E}[X]$ let to define the pure premium PP by adding the safety loading δ

$$PP = \mathbb{E}[X] + \delta.$$

The sum of the pure premium and the expense loadings gives the expenses-loaded premium

$$EP = \frac{PP}{(1-\eta)}. \tag{9}$$

The expense loading proportion is denoted by η and is measured in EP. The safety loading δ_{CoC} is determined according to the principle of the cost of capital (CoC). Let ρ be the cost of capital rate, assuming that the risk will expire in one year, the target solvency ratio is equal to ξ% and $i_{rf(0,1)}$ is the risk-free rate between 0 and 1, then we define δ_{CoC} as

$$\delta_{CoC} = \frac{\xi\rho \cdot SCR}{\left(1 + i_{rf(0,1)}\right)} = \frac{\xi\rho \cdot [VaR_{\alpha\%}(X) - \mathbb{E}[X]]}{\left(1 + i_{rf(0,1)}\right)}.$$

The relationship among risks is a crucial point for a correct definition of capital requirements and the expense-loaded premium. As highlighted by Adelmann et al. (2020), there is an interconnection between cyber risk and financial stability, through knock-on effects that affect financial operators and institutions, which arises through a loss of confidence by lead customers, lack of liquidity, and substitutability, which can be emphasised by weaknesses in technology and communications between technology and financial operators. For these reasons, many studies focus on the interaction effects between cyber attacks and the impact on the assessment of capital requirements and the pricing of insurance products.

In particular, Eling and Schnell (2020) proposed an empirical analysis comparing the results of Solvency II, the US Risk-Based Capital Standards, and the Swiss Solvency Test regulations for the calculation of capital requirements, considering the correlations between sources of risk. In the paper, the fallacy of independence emerges: treating each risk as independent (e.g., the sum of individual risks with marginal distributions) leads to underestimating the aggregate risk. Copulas are used precisely to model this dependence between events, separating the dependence structure from the marginal distributions. The theoretical basis for the use of copulas is provided by Sklar's theorem, which states that for every multivariate distribution $H(x_1, \ldots, x_d) = \mathbb{P}(X_1 \leq x_1, \ldots, X_d \leq x_d)$ of a random vector $X = (X_1, \ldots, X_d)$ with marginal distributions $F_i(x) = \mathbb{P}(X_i \leq x_i)$, there exists a copula C such that

$$H(x_1, \ldots, x_d) = C(F_1(x), \ldots F_d(x)).$$

Additionally, the converse is true. Given a copula $C : [0,1]^d \to [0,1]$ and marginals $F_i(x)$, then $C(F_1(x_1), \ldots, F_d(x_d))$ defines a $d-$dimensional cumulative distribution function with marginal distributions $F_i(x)$. The main families of Copula are elliptical and Archimedean.

For a random vector X which expectation and variance are constant, let $\psi : [0, \infty) \to \mathbb{R}$ be a function such that $\phi_{X-\mu} = \psi(t'\Sigma t)$. If it holds for the characteristic function $\phi_{X-\mu}$ of $X - \mu$, X is an elliptically distributed random vector with parameters μ, Σ, and ψ. To isolate the dependence structure, we define $u_i = F_i(x_i)$, for $i = 1, \ldots, d$, so that $u = (u_1, \ldots, u_d) \in [0,1]^d$ is a vector of standardised uniform variables. Let $X \sim Ed(\mu, \Sigma, \psi)$ be an elliptically distributed random vector with the cumulative distribution function H and continuous marginal distributions $F_i(x)$. The unique copula C of X with $C(u) = H(F_1^{-1}(u_1), \ldots, F_d^{-1}(u_d))$ is called an elliptical copula. The most well-known and commonly used elliptical copulas are the Gaussian copula with correlation matrix R and the t-copula, namely

$$C_R^{\text{Gauss}}(u) = \Phi_R^d(\phi^{-1}(u_1), \ldots, \phi^{-1}(u_d)),$$

where Φ_R^d is the cumulative density function of a d-dimensional normal distribution with expected vector 0 and correlation matrix R, and ϕ^{-1} is the inverse of the standard normal marginal distribution.

$$C_{\alpha,R}^t(u) = t_{\alpha,R}^d(t_\alpha^{-1}(u_1), \ldots, t_\alpha^{-1}(u_d)),$$

where $t_{\alpha,R}^d$ is the cumulative density function of $\frac{\sqrt{\alpha}}{\sqrt{S}}Z$, where $S \sim \chi_\alpha^2$, $Z \sim N_k(0, R)$, and S and Z are independent. t_α are the marginal distributions of $t_{\alpha,R}^d$.

Elliptic copulas are symmetric and characterised by a linear dependence structure. The main difference between a Gaussian and t-copula is that the former has zero asymptotic dependence in the tails, while the latter shows symmetric and positive tail dependence. The main disadvantages of elliptical copulas are the inability to handle asymmetric relationships

and the absence of a general closed form, overcome by Archimedean copulas. Let $\mathcal{F}$: $[0,1] \to [0,+\infty]$ be a continuous, strictly monotone decreasing function with $\mathcal{F}(1) = 0$. The pseudo-inverse function $\mathcal{F}^{[-1]} : [0,+\infty] \to [0,1]$ is defined by

$$\mathcal{F}^{[-1]}(t) = \begin{cases} \mathcal{F}^{-1}(t) & 0 \leq t \leq \mathcal{F}(0) \\ 0 & \mathcal{F}(0) \leq t \leq +\infty \end{cases}.$$

$\mathcal{F}^{-1}(t)$ is continuous and monotone decreasing on $[0,\infty]$, strictly monotone decreasing on $[0,\mathcal{F}(0)]$ and $\mathcal{F}^{[-1]}(\mathcal{F}(u)) = u$ for $u = [0,1]$ holds. The function $C : [0,1]^d \to [0,1]$, with $C(u;\mathcal{F}) = \mathcal{F}^{[-1]}(\mathcal{F}(u_1),\ldots,\mathcal{F}(u_d))$ is a copula if $\mathcal{F}$ is convex, and C is an Archimedean copula with generator $\mathcal{F}$. Also of note, Archimedean copulas are as follows: Gumbel copula, with $\mathcal{F}(t) = (-\ln t)^\theta, \theta \geq 1$ to model right tail dependence, Clayton copula, with $\mathcal{F}(t) = \frac{1}{\theta}(t^{-\theta} - 1), \theta > 0$, to model left tail dependence, and Frank copula, with $\mathcal{F}(t) = -\ln\left(\frac{\exp(-\theta t)-1}{\exp(-\theta)-1}\right), \theta \neq 0$ to model symmetric dependence. To model the loss linked to insurance company solvency, Eling and Schnell (2020) used a Clayton copula to show that even small changes in the copula model or parameters lead to significant changes in the expected rewards and benefits from diversification, with an underestimation of capital requirements for cyber risk hedging, especially for small portfolios. In a previous research, Eling and Jung (2018) performed a Pair Copula Construction, which is an approach to combine bivariate copulas according to a criterion, in this case, the type of breach and business sectors, to show the presence of an asymmetric tail dependency structure among cyber attacks. In this way, the model describes correlations between extreme losses much more realistically than simpler or independent models. Mukhopadhyay et al. (2013) proposed a Copula-Bayesian Vulnerability Assessment, combining a Bayesian Belief Network and a Gaussian copula to assess the vulnerability of computer security systems to attacks and the convenience of associating the investment in security with an insurance hedging. Xu et al. (2018) analysed the dependency structure between frequency and severity of cyber attacks, comparing different types of copulas, both elliptical and Archimedean, showing that the inter-arrival periods of the breaches and the breach magnitude are positively correlated. According to the cybersecurity definition of reliance, a significant breach is more likely to occur after a prolonged period without any occurrences. Based on this result, they propose a stochastic loss forecasting process that takes into account both severity and frequency. In a later research, Xu and Hua (2019) integrates Gaussian and Clayton copulas into non-Markovian models, which takes into account the relationship between waiting time and severity of an attack, while also including network contagion effects. In this way, the model takes into account both time dependence and network contagion effects. The results show that non-Markovian models, in combination with copulas, are able to model the simultaneity of attacks and the persistence of the threat, which Markovian models tend to underestimate. Carannante et al. (2023) focused on the dependency structure of breaches, using vine copulas by type of attack. Vine is a tool to define constraints in high-dimensional probability distributions. In particular, decomposing the multivariate copula $C(u)$ into a sequence of conditional bivariate copulas allows for a more flexible representation of dependence structures. In other words, a vine copula expresses $C(u)$ as the product of conditional bivariate copulas. In particular, (F,V,B) denotes a vine copula specification where $F = (F_1,\ldots,F_d)$ is a vector of continuous invertible marginal distribution functions, and $B = \{B_e | i = 1,\ldots,d-1; e \in E_i\}$ is a set of copulas with B_e being a bivariate copula. The unique specification of the vine copula, whose density is given by

$$f_{1\ldots d}(x) = \prod_{k=1}^{d} f_k(x_k) \prod_{i=1}^{d-1} \prod_{e \in E_i} c_{C_{e,a},C_{e,b}|D_e}\left(F_{C_{e,a}|D_e}\left(\mathbf{x}_{C_{e,a}}|\mathbf{x}_{D_e}\right), F_{C_{e,b}|D_e}\left(\mathbf{x}_{C_{e,b}}|\mathbf{x}_{D_e}\right)\right)$$

where $\mathbf{x} = (x_1, \ldots, x_d)$, $e = \{a, b\}$, $x_{D_e} = \{x_i | i \in D_e\}$, and $c_{C_{e,a},C_{e,b}|D_e}$ is the bivariate copula density for edge $e = \{a, b\}$. The advantage of using vine copulas is to identify the type of relationship that occurs between the random variables by comparing them in pairs. Carannante et al. (2023) showed that the vine copula approach outperforms elliptical multivariate copulas in a prudential sense to determine the SCR in a cyber risk hedging framework, analysing the relationship among seven cyber breaches. Peng et al. (2018) proposed a combined vine copula and GARCH approach to model the volatility of breaches on individual servers and their dependencies. Empirical results show that this Copula-GARCH approach improves the accuracy of predicting joint risk exposure, allowing for better estimation of indicators such as multivariate Value-at-Risk. Cherubini (2024) extended the GL1 model in Equation (1) to the multivariate case using vine copulas to model the losses deriving from a multiple attack or addressed to multiple technologies. On a similar front, Bardopoulos (2025) analysed the dependency relationships between risks related to cyber attacks, comparing different heavy-tailed loss functions and estimating the joint distributions of loss. The empirical analysis shows that the main risk factor is the tail volatility, which insurance companies do not take into account in their assessments, leading to an underestimation of capital requirements. Ballestra et al. (2024) evaluates a different aspect of interdependency, namely the geographical basis risk in the cyber insurance products due to contagion effects. A breach risk model based on a count regression that combines exchangeable random effects and spatial random effects is proposed to determine the risk of breach in the US. The empirical analysis shows the opportunity to propose a generalised scheme to ensure most of the US states are covered.

4.2. Cyber Insurance Products

Cyber insurance is a risk management tool that has become increasingly important in response to the spread and danger of cyber attacks, especially in the context of businesses and critical infrastructures. It represents a form of risk transfer in which an organisation takes out a policy t,o hedge economic losses due to breaches, business interruptions or reputational damage. However, despite the increasing demand in recent years, the cyber insurance market remains limited compared to other insurance areas, partly due to the high uncertainty in assessing and pricing cyber risk. The barriers that limit the growth of cyber insurance are of interest to international organisations. In particular, Organisation for Economic Co-operation and Development (2017) stated the need to overcome structural barriers in the insurance market, including the scarcity of historical data, regulatory uncertainty, and the difficulty of modelling the systemic risk associated with large-scale attacks. Organisation for Economic Co-operation and Development (2020) also highlighted the need to make insurance hedging more transparent and understandable, both for policyholders and insurers, suggesting regulatory tools to improve contractual clarity and encourage the spread of policies. Weber et al. (2024) analysed actuarial techniques and applications of artificial intelligence in cyber risk assessment, identifying potential tools to improve the underwriting and pricing process. Barreto et al. (2021) focused on the specific challenges posed by cyber-physical systems, such as energy infrastructure, industrial plants, and intelligent transport, where the consequences of an attack can propagate into the physical world and cause catastrophic damage, highlighting the difficulties in risk assessment for cyber-physical systems. A possible solution could be a combination of insurance innovation and regulatory intervention to encourage transparency and develop tools appropriate to the

complex nature of these systems. One of the aspects that limits the growth of the insurance market is the presence of moral hazards and information asymmetries. Shetty et al. (2010) proposed a market competitive model for insurance companies, showing that the lack of information about the level of investment in cybersecurity by insurance companies causes market inefficiency, as this depends on the utility functions of individual policyholders. In addition, there is a moral hazard effect, as insurance coverage discourages investments in security. In particular, the goal is to optimise both policyholders' and insurance companies' utility. Let $s \geq 0$ be the cybersecurity investment to minimise the expected costs; insurance companies compete by offering premiums $EP(s)$ and indemnity share $\delta \in [0,1]$. The expected utility for the policyholder is given by

$$\mathcal{U}(s) = -EP(s) - \mathbb{P}(s) \cdot (1-\delta)L - \mathcal{C}(s)$$

where $EP(s)$ is the insurance premium to pay (expenses-loaded premium), $\mathbb{P}(s)$ is the loss probability, L is the economic value of the loss, and $\mathcal{C}(s)$ is the cost of investment in cybersecurity. The insurance companies' problem is to maximise their profit, given the rational behaviour of the user and the competition in the market

$$\max_{EP,\delta} \{EP(s) - \mathbb{P}(s) \cdot \delta L\}.$$

The lack of information about the level of investment s in cybersecurity by insurance companies is a cause of market inefficiency. In addition, there is a moral hazard effect, as insurance coverage discourages investments in security. The analysis shows that it is not possible to optimise both policyholders' utility and insurance companies' profits. Romanosky et al. (2019) systematically analysed over 100 cyber insurance policies collected from US state commissioners, identifying four main areas evaluated by insurers: governance and compliance; technical; internal policies and procedures; and regulatory aspects. On the pricing front, the authors highlight strong heterogeneity. Many policies adopt a flat-rate model based exclusively on the asset value or turnover of the company, ignoring security controls. Only about a third of companies integrate factors related to the actual security status of the insured into the premium calculation. Many premiums remain approximate and poorly correlated with the actual security of the insured, indicating a potential benefit in integrating more granular technical assessments into the underwriting processes. Zeller and Scherer (2022) proposed a quantitative formalisation for a cyber insurance contract through a marked point process, which allows for overcoming the main limitations of cyber insurance. In particular, instead of relying on static or heuristic premiums, they directly model the distribution of losses, allowing pricing based on real risk. Their model can be used both by insurers and by regulators, bridging a gap between actuarial theory and commercial practice. In particular, the stochastic process is defined as a sequence of marked points

$$\{(t_i, (m_i, S_i))\}_{i \in \mathbb{N}} \subset [0,T] \times (M \times \mathcal{P}(\{1,\ldots,J\}))$$

where t_i is the arrival time, $m_i \in [m_{\min}, m_{\max}]$ is a mark to describe severity and frequency, and $S_i \subseteq \{1,\ldots,J\}$ is the set of breached firms in portfolio. Marks (m_i, S_i) are independent from arrival time t_i, that is

$$(m_i, S_i) \perp t_i \quad \text{for each } i \in \mathbb{N}.$$

The main advantage of this approach is considering cyber interdependencies from a dynamic perspective. Xiang et al. (2024) determined a dynamic equilibrium for cyber insur-

ance contracts, introducing a Bonus–Malus system to incentivise risk reduction through autonomous mitigation measures and reduce moral hazard by rewarding those who do not file claims or adopt good practices. In particular, a Markov transition model is defined to update dynamically the insurance state to calculate the premium. For $t = 1, \ldots, T$, let $f_t : \mathcal{B}_1 \times \mathcal{B}_2 \times \mathcal{D} \times \{0,1\} \times \{0,1\} \times \mathcal{W} \to \mathcal{B}_1 \times \mathcal{B}_2$ be the state transition function for each year t, given by

$$f_t(b_1, b_2, d, \iota, j, w) := \begin{cases} \mathcal{BM}\big(b_1, j\lambda^{\mathcal{BM}}(b_1, t, L(d, w))\big), & \text{if } \iota = 1, \\ \mathcal{BM}_0(b_1, b_2), & \text{if } \iota = 0, \end{cases}$$

where $\lambda^{\mathcal{BM}}$ is the Bonus–Malus loss function. In other words, $f_t(b_1, b_2, d, \iota, j, w)$ returns the Bonus–Malus level and the insurance state in year t given that the Bonus–Malus level and the insurance state in year $t-1$ are b_1 and b_2, the decisions in year t are d, ι, j, and the cyber loss events in year t are w. Chong et al. (2025a) developed an economic basis for incident-specific cyber insurance products, focusing on how incident-specific benefits should be designed to achieve Pareto optimality for both the insurance seller and the buyer. Real-world cyber incident data is used to illustrate the feasibility of this approach. Additionally, several implementation improvement methods are discussed for practicality. In particular, the expected utility of the insured, considering the specific coverage for the type of accident, can be expressed as

$$\mathcal{U} = \mathbb{E}\left[u\big(\mathrm{W} - EP - \sum_k \mathrm{I}_k \cdot L_k\big)\right]$$

where W is the initial wealth, EP the insurance premium paid, $\mathrm{I}_k \in \{0,1\}$ indicates whether the accident of type k is hedged, L_k is the loss associated with the accident of type k, and $\mathcal{U}$ is the utility function of the policyholder. The premium and hedging structure I_k is designed to achieve a Pareto efficient equilibrium between insurer and insured for each type of accident. Finally, Chong et al. (2025b) introduced a two-pillar cyber risk management framework to address the pervasive challenges in cyber risk management. The first pillar, cyber risk assessment, combines insurance frequency–severity models with cybersecurity cascade models to capture the unique nature of cyber risk. The second pillar, cyber capital management, facilitates informed capital allocation for a balanced cyber risk management strategy, including cybersecurity investments, insurance coverage, and reserves. A case study, based on historical cyber incident data and realistic assumptions, demonstrates the need for a comprehensive cost–benefit analysis for companies with limited budgets and competing cyber risk management objectives. Additionally, a sensitivity analysis highlights the dependence of the optimal strategy on factors such as the price of cybersecurity controls and their effectiveness. The optimal capital management is formalised as the following minimisation problem:

$$\min_{\mathcal{C},\mathrm{I},CoC} \{\mathcal{C} + EP(\mathrm{I}) + CoC(\mathcal{R})\}$$

subject to

$$\mathbb{P}(X > \mathcal{R} + \mathrm{I}) \leq \alpha$$

where $\mathcal{C}$ is cybersecurity investments, I is the level of insurance coverage, $\mathcal{R}$ is capital reserves, $EP(\mathrm{I})$ is the insurance premium as a function of I, $CoC(\mathcal{R})$ is the cost of capital associated with reserves, and α is the level of acceptable risk (e.g., VaR or probability of default).

4.3. Cyber Reinsurance

Insurance companies employ cyber reinsurance as a safeguard to control their exposure to cyber threats (Cremer et al. 2024). Insurers who provide specialised coverage for cyber risks—like ransomware attacks, data breaches, or disruptions of digital services—are more vulnerable to potentially significant and frequently unanticipated losses as a result of the growth in these threats. In order to safeguard themselves, they assign a portion of this risk to reinsurance firms, who then distribute it among a larger and more varied portfolio (Woods and Wolff 2025). Since cyber risks are different from other insurance categories, reinsurance is especially crucial in this situation. A single cyber attack can disrupt hundreds of businesses at once, particularly if they depend on shared cloud services or software providers. This is the first example of how cyber incidents can have a systemic effect. Furthermore, the very nature of cyber risk is ever-changing: new vulnerabilities appear on a regular basis, making it challenging to forecast with precision how frequently and how severe accidents will occur. Risk piling, which means that a single incident might affect several policies, is another important problem. An insurance company's decision to keep the entire exposure on its own balance sheet is, therefore, dangerous. It is consequently more practical to provide cyber coverage in the market since reinsurance permits risk pooling and diversification. The need for cyber reinsurance has increased dramatically in recent years, but reinsurers are being cautious. Cyber risk is one of the most complicated issues facing the insurance industry as a whole because of the dearth of adequate historical data, the high degree of uncertainty, and the possibility of catastrophic catastrophes Zängerle and Schiereck (2023). In this context, alternative risk transfer mechanisms such as cyber catastrophe bonds (cat bonds) have been proposed as innovative reinsurance tools. As discussed in Mastroeni et al. (2022), cyber cat bonds can help insurers transfer part of their cyber risk exposure to capital markets, offering a potential solution to the capacity constraints and uncertainty inherent in traditional reinsurance models. These instruments could play a key role in enhancing the resilience of the cyber insurance ecosystem by enabling broader risk sharing and attracting new sources of capital.

5. Pricing

This section presents several models proposed in the scientific literature for determining insurance premiums in the context of cyber insurance. In particular, we describe the mathematical models and the variables commonly used for this purpose. An early discussion surrounding the role of insurance in cybersecurity focused on its potential to incentivise security investments—specifically, whether insurance promotes increased investment in protection or instead gives rise to a "market for lemons." Proponents of cyber insurance include Kesan et al. (2004), Bolot and Lelarge (2009), and Yang and Lui (2014), particularly in scenarios where protection quality is not sufficiently high. On the other hand, critics such as Pal et al. (2014) and Shetty et al. (2010) argue that significant information asymmetry regarding the policyholders' actual vulnerability prevents the emergence of a viable insurance market. Key challenges to the adoption of cyber insurance—namely, asymmetric information and correlated risks—were already identified by Baer and Parkinson (2007) and continue to persist today. As previously highlighted, identifying an appropriate distribution for cyber claims is extremely challenging. Several studies, including Edwards et al. (2016), highlighted the absence of a well-defined distribution for such events. As a result, increasingly sophisticated models are required to minimise the risk of loss estimation errors and, consequently, to optimise pricing models (Adriko and Nurse 2024; Franke 2017). In the paper by Böhme and Kataria (2006), premiums were not determined exogenously; rather, they depend on the expected expenditure incurred by insurance companies to settle

all claims within a given period. The total cost TC for insurers in a single period can be expressed as the sum of three components:

$$TC = \mathbb{E}[X] + Admin + r \cdot Sc$$

where $\mathbb{E}[X]$ is the expected value of the loss, with X representing a random variable denoting the exposure to risk distribution, $Admin$ is the total administrative cost, which is assumed to be negligible, Sc denotes the amount of safety capital required to ensure full coverage in the event that the realised losses exceed expectations, and r is the interest rate applied to the safety capital Sc, reflecting the risk profile of the insurance business. With reference to Equation (9), TC corresponds to the expenses-loaded premium EP recalculated for each period. Lau et al. (2020) analysed the insurance premium using the well-known Expected Value Premium Principle (see for details Kaas et al. 2008), which defines the pure premium as being proportional to the expected loss. However, they assess that this approach is not suitable for cyber risks, as these risks are typically not independent. Specifically, it is defined as follows:

$$PP = (1 + \lambda)\mathbb{E}[X]$$

where X is the random variable describing the potential total loss and λ is the risk loading coefficient. In this model, the Risk loading coefficient is set to a positive value to account for uncertainty, cover administrative costs, and ensure a profit margin. However, it is typically kept relatively low to maintain the affordability of the insurance product. To address the dependency among risks, the authors introduce a more advanced approach for insurance premium calculation. Given the total potential loss across all Transmission Companies in the energy sector, defined as

$$X = \sum_{i=1}^{n} X_i,$$

they propose determining the pure premium using Value-at-Risk (VaR). This method sets the premium as

$$PP_1 = VaR_\alpha(X)$$

where $\alpha \in (0, 1)$ represents the chosen confidence level. The key idea is to ensure that the probability of the total loss exceeding the premium remains within acceptable bounds, specifically

$$\mathbb{P}(X > PP_1) = \alpha.$$

Since VaR only considers the threshold beyond which extreme losses occur, the authors further propose a more conservative alternative based on Tail Value-at-Risk (TVaR). This measure accounts for the average loss in the tail beyond the VaR threshold and is given by

$$PP_2 = TVaR_\alpha(X) = \frac{1}{\alpha}\int_0^\alpha VaR_y(X)\, dy.$$

This approach provides a stronger guarantee, ensuring that the probability of losses exceeding the premium is strictly less than the confidence level α, $\mathbb{P}(X > PP_2) < \alpha$.

Lin et al. (2018), in their paper, employed the extension of the expected value premium principle known as the mean–variance premium (see, for example, Olivieri and Pitacco 2015) to compute the price of the cyber insurance premium. In particular, they defined the pure premium as follows:

$$PP = \mathbb{E}[X] + \frac{\delta}{2}\mathbb{V}[X],$$

where δ is the risk aversion coefficient, and is using the random variable of the exposure risk $X = \sum_{i=1}^{N} L$ where N is the number of records breached and L is the random variable of loss. Specifically, starting from Equation (8), the pure premium is defined as

$$PP = \mathbb{E}[N]\mathbb{E}[L] + \frac{\delta}{2}(\mathbb{E}^2[L] + \mathbb{V}[L])\mathbb{E}[N].$$

The mean–variance premium was also used by Mastroeni et al. (2019) to determine the total insurance premium for service disruptions occurring in the cloud, using three different metrics for claims: service disruption, prolonged disruption, and service time unavailability. A similar model was used by Antonio et al. (2021). In particular, authors employed the standard deviation principle to compute the insurance premium

$$PP = \mathbb{E}[X] + \delta\sqrt{\mathbb{V}[X]}.$$

The standard deviation principle differs from the mean–variance premium principle primarily in its use of the standard deviation, rather than the variance, in the pricing formula (see also Bühlmann 1970). This substitution results in a comparatively lower sensitivity to the risk associated with the underlying random variable. Specifically, Antonio et al. (2021), using this principle, found that, defining by L and R the loss and the system downtime, the random variable of the total loss X is defined as

$$X = \sum_{i=1}^{N}(\mu(L) + \gamma(R))$$

where N is the number of infections, μ the cost function due to infection, and γ is the cost function corresponding to the length of time-to-repair. So, the pure premium is defined by the following equation:

$$PP = \mathbb{E}\left[\sum_{i=1}^{N}(\mu(L) + \gamma(R))\right] + \delta\sqrt{\mathbb{V}\left[\sum_{i=1}^{N}(\mu(L) + \gamma(R))\right]}.$$

In the paper by Lau et al. (2021), the authors proposed a cooperative framework for cyber insurance premium calculation, specifically applied to the power sector. The model is based on the formation of a coalition among multiple Transmission Operators that jointly share cyber risk. The premium was computed by estimating the expected economic losses resulting from cyber attacks, taking into account both cyber vulnerability and the impact on power system reliability. This was achieved through stochastic simulations that model load loss and translate it into monetary terms. The pure premium for the coalition was given by

$$PP_{\text{coalition}} = \mathbb{E}[L_{agg}] + \lambda\sqrt{\mathbb{V}[L_{agg}]}$$

where $\mathbb{E}[L_{agg}]$ denotes the expected value of aggregated losses. The premium is then fairly allocated among the coalition members using the Shapley value, which reflects each operator's marginal contribution to the total risk. This approach promotes risk sharing, incentivises cooperation, and enables more accurate and sustainable cyber insurance pricing for interdependent power systems. On the other hand, Mukhopadhyay et al. (2013, 2019) computed the pure premium PP_i for insuring against each type of cyber attack, calculating it as the expected severity $\mathbb{E}(L_i)$ of each attack L_i, multiplied by the overhead loading OV, plus the standard deviation of the loss of each attack $\sqrt{\mathbb{V}(L_i)}$ multiplied by the contingency loading k

$$PP_i = OV \cdot \mathbb{E}(L_i) + k\sqrt{\mathbb{V}(L_i)}.$$

Building on the mean–variance premium principle, Naldi and Mazzoccoli (2018) proposed an extended approach, which was subsequently employed by Mazzoccoli and Naldi (2020b), involving the use of higher-order moments—up to the fourth order—in the determination of pure premiums

$$PP = \mathbb{E}[X] + \frac{\delta}{2}\mathbb{V}[X] + \frac{\delta^2}{6}\mathbb{S}[X]\mathbb{V}^{3/2}[X] + \frac{\delta^3}{24}\mathbb{K}[X]\mathbb{V}^2[X]$$

where, in this case, δ is the constant absolute risk aversion coefficient defined as in Babcock et al. (1993)[1]:

$$\delta = \frac{1}{\mathbb{E}[X]} \ln\left(\frac{1+2\varepsilon}{1-2\varepsilon}\right)$$

where $\varepsilon \in (0, \frac{1}{2})$ is the probability premium. The use of statistical moments up to the fourth order—such as skewness and kurtosis—allows for a more accurate representation of the risk distribution, especially in the presence of heavy tails or asymmetric distributions. In many cases, the fourth-order premium tends to be higher than the second-order (mean–variance) approximation, providing greater protection against extreme events. The model accounts not only for variability (second moment) but also for the shape of the risk distribution (third and fourth moments), enabling a more sophisticated pricing approach. However, higher-order moments (third and fourth) are significantly more difficult to estimate accurately, particularly when dealing with small or noisy datasets. Estimation errors in these moments can lead to distorted premium values. Moreover, the dispersion of the premium calculated using the fourth-order approximation can be substantial; in some cases, it may result in excessively high premiums that are not justified by an actual increase in risk exposure. Another pricing model was introduced by Mazzoccoli and Naldi (2020a). In particular, they defined the pure premium in a different way using the Gordon and Loeb model for the vulnerability

$$PP = kpL(1 - r(1 - v))$$

where k is the premium rate coefficient, p is the attack probability, L is the loss, and v is the vulnerability described by Equations (1) and (2). As can be seen, this formulation is adaptable to any vulnerability model expressed through Equations (3)–(7). An extension of this model was used by Mazzoccoli and Naldi (2021) for a multi-branch firm under a full set of insurance liability scenarios, that is, full coverage, limited coverage, and limited coverage of the losses with deductibles. In this case, the authors used a vulnerability function

$$v = 1 - (1 - pv_0)\prod_{i=1}^{m}(1 - \rho v_i)$$

where v_0 is the vulnerability of a firm (called principal firm or headquarters), v_i is the vulnerability of the i-th firm risk-connected with the principal firm, and m is the number of risk-connected firms with the principal firm. Moreover, the model proposed by Mazzoccoli and Naldi (2020a) has also been employed in the paper by Mazzoccoli and Naldi (2022b) with the introduction of a time-dependent vulnerability function. In particular, the authors model vulnerability as following a sawtooth pattern: it increases over time within each interval (t_{i-1}, t_i), but is sharply reduced at the moments when investments are made,

namely at times $t_1, t_2, \ldots, t_n$. During the intervals between investments, the evolution of vulnerability is described by a logistic function

$$v(t) = \frac{v_0}{1 + e^{-\xi(t-\tau)}} \quad \text{for } t_i < t < t_{i+1}.$$

Here, v_0 represents the maximum possible vulnerability, ξ is the logistic growth rate (i.e., the steepness of the curve), and the parameter

$$\tau = t_{i+1} - \frac{1}{\xi} \ln\left(\frac{v_0}{v(t_i)} - 1\right)$$

is determined based on the vulnerability level just after the most recent investment.

Herath and Herath (2007, 2011), to compute the insurance premium, previously described the random variable of total loss L as

$$L = \begin{cases} c_1 \quad if \quad n \leq n_1 \\ c_2 + \frac{n-n_1}{n} \frac{l}{10} \quad if \quad n_1 < n < n_2 \\ c_3 + \frac{n-n_2}{n} \frac{l}{10} \quad if \quad n \geq n_2 \end{cases}$$

where l is the random variable representing the economic loss, n is the random variable describing the number of computers affected, n_1 and n_2 are the lowest and highest limits of the numbers of likely computers affected, and c_1, c_2, and c_3 are three constants. After describing the total loss, they formulate the pure premium in the following way:

$$PP = \begin{cases} 0 \quad if \quad L \leq ded \\ (1 - c^*)(L - ded) \quad if \quad d < L < d + \frac{l^*}{1-c^*} \\ l^* \quad if \quad L > d + \frac{l^*}{1-c^*} \end{cases}$$

where *ded* are the deductibles, l^* is the limit of coverage, and c^* is the coinsurance.

An outline of the main methods and models for insurance premium calculation is provided in Table 2.

The analytical frameworks discussed here not only extend traditional approaches but also highlight the need for ongoing refinement to address emerging cyber threats and evolving market dynamics. These considerations pave the way for future research and practical applications, which we summarise in the final conclusions.

Table 2. Summary of the fundamental principles of cyber insurance premium calculation. X is the random variable representing the loss, and λ is a positive real constant.

Principle	**Mathematical Formulation**
Expected value premium	$PP = (1 + \lambda)\mathbb{E}[X]$
Mean-variance premium	$PP = \mathbb{E}[X] + \frac{\lambda}{2}\mathbb{V}[X]$
Standard deviation premium	$PP = \mathbb{E}[X] + \frac{\lambda}{2}\sqrt{\mathbb{V}}[X]$
Fourth order statistics	$PP = \mathbb{E}[X] + \frac{\lambda}{2}\mathbb{V}[X] + \frac{\lambda^2}{6}\mathbb{S}[X]\mathbb{V}^{3/2}[X] + \frac{\lambda^3}{24}\mathbb{K}[X]\mathbb{V}^2[X]$
Tail Value-at-Risk premium	$PP = \frac{1}{\alpha}\int_0^\alpha VaR_y(X)\, dy.$

6. Conclusions

This article proposed an overview of the field of cyber insurance, focusing on the mathematical models used to measure cyber risk in terms of losses due to cyber attacks, the effects of interdependency of risk, both in a temporal or spatial dimension, and among

types of breaches, on pricing and capital requirements. We started by analysing the main ways to describe cyber risks, such as key vulnerability functions and different stochastic and dynamic models that show the unique characteristics of cyber threats. Next, we gave an overview of the cyber insurance market, focusing on the regulatory issues, the characteristics of insurance products to hedge cyber risk analysed in academic literature, and the role of cyber reinsurance, and looked at the main pricing models that have been suggested in the literature for figuring out how much to charge for insurance.

Our research shows that even though modelling techniques and pricing strategies have come a long way, there are still some problems that need to be solved. Some of these are the problems with accurately measuring changing and evolving threats, managing risks that are related to each other, and dealing with the fact that insurers and insured parties do not always have the same information. Furthermore, the lack of standardised methods and data-sharing practices hinders the development of more precise pricing models and limits the overall efficiency of the cyber insurance market.

These open questions show that we need to do more research on adaptive pricing systems, better risk assessment tools, and frameworks that better incorporate new technologies like real-time monitoring and threat intelligence. It is also important to close the gap between theoretical models and real-world use to make sure that cyber insurance not only protects against financial losses but also encourages better cybersecurity practices.

Finally, we emphasise that closer collaboration between researchers, insurers, and policymakers will be crucial to overcoming these challenges and fostering the sustainable growth of the cyber insurance market as an effective risk management tool in an increasingly digital society.

Looking ahead, future research could focus on developing innovative actuarial models that better capture the unique characteristics of cyber risk, including its rapid evolution and systemic nature. Further work could also explore new forms of reinsurance structures for cyber risk, the use of advanced data analytics and artificial intelligence to enhance risk prediction, and the design of regulatory frameworks that encourage information sharing and market resilience. Such research directions would contribute to making cyber insurance a more robust and adaptive instrument for managing the complex and ever-changing landscape of cyber threats.

Author Contributions: Conceptualization, A.M. and M.C.; formal analysis, A.M. and M.C.; investigation, A.M. and M.C.; writing—original draft preparation, A.M. and M.C.; writing—review and editing, A.M. and M.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing is not applicable. No new data were created or analyzed in this study.

Conflicts of Interest: The authors declare no conflicts of interest.

Note

[1] The coefficient δ can also be defined as $\beta = \frac{1}{\mathbb{E}[X]}$, see Olivieri and Pitacco (2015). This coefficient coincides with the coefficient introduced by Babcock et al. (1993) when $\varepsilon = \frac{e-1}{2(1+e)}$.

References

Abou El Houda, Zakaria. 2024. Cyber threat actors review: Examining the tactics and motivations of adversaries in the cyber landscape. In *Cyber Security for Next-Generation Computing Technologies*. Boca Raton: CRC Press, pp. 84–101.

Adelmann, Frank, Jennifer Elliott, Ibrahim Ergen, Tamas Gaidosch, and Nigel Jenkinson. 2020. *Cyber Risk and Financial Stability: It's a Small World after All*. Washington, DC: International Monetary Fund.

Adriko, Rodney, and Jason R. C. Nurse. 2024. Cybersecurity, cyber insurance and small-to-medium-sized enterprises: A systematic review. *Information & Computer Security* 32: 691–710.

Allianz Commercial. 2025. Allianz Risk Barometer 2025: Identifying the Major Business Risks for 2025. Available online: https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html (accessed on 2 July 2025).

Antonio, Yeftanus, Sapto Wahyu Indratno, and Suhadi Wido Saputro. 2021. Pricing of cyber insurance premiums using a markov-based dynamic model with clustering structure. *PLoS ONE* 16: e0258867. [CrossRef] [PubMed]

Aven, Terje, Yakov Ben-Haim, H. Boje Andersen, Tony Cox, Enrique López Droguett, Michael Greenberg, Seth Guikema, Wolfgang Kröger, Ortwin Renn, Kimberly M. Thompson, and et al. 2018. *Society for Risk Analysis Glossary.* Herndon: Society for Risk Analysis.

Awiszus, Kerstin, Thomas Knispel, Irina Penner, Gregor Svindland, Alexander Voß, and Stefan Weber. 2023. Modeling and pricing cyber insurance: Idiosyncratic, systematic, and systemic risks. *European Actuarial Journal* 13: 1–53. [CrossRef]

Babcock, Bruce, Kwan Choi, and Eli Feinerman. 1993. Risk and probability premiums for cara utility functions. *Journal of Agricultural and Resource Economics* 18: 17–24.

Baer, Walter S., and Andrew Parkinson. 2007. Cyberinsurance in it security management. *IEEE Security & Privacy* 5: 50–56. [CrossRef]

Ballestra, Luca, D'Amato Valeria, Fersini Paola, Forte Salvatore, and Greco Fedele. 2024. Pricing cyber insurance: A geospatial statistical approach. *Applied Stochastic Models in Business and Industry* 40: 1365–76. [CrossRef]

Bardopoulos, James. 2025. Cyber-insurance pricing models. *British Actuarial Journal* 30: e6. [CrossRef]

Barreto, Carlos, Galina Schwartz, and Alvaro A. Cardenas. 2021. *Cyber-Insurance*. Cham: Springer International Publishing, Chapter 15, pp. 347–75. [CrossRef]

Bolot, Jean, and Marc Lelarge. 2009. Cyber insurance as an incentive for internet security. In *Managing Information Risk and the Economics of Security*. Cham: Springer, pp. 269–90.

Böhme, Rainer, and Gaurav Kataria. 2006. Models and measures for correlation in cyber-insurance. *Weis* 2: 3.

Bühlmann, Hans. 1970. Premium calculation. *Mathematical Methods in Risk Theory* 85–110.

Callegaro, Giorgia, Claudio Fontana, Caroline Hillairet, and Beatrice Ongarato. 2025. A stochastic gordon-loeb model for optimal cybersecurity investment under clustered attacks. *arXiv* arXiv:2505.01221. [CrossRef]

Carannante, Maria, Valeria D'Amato, Paola Fersini, Salvatore Forte, and Giuseppe Melisi. 2023. Vine copula modeling dependence among cyber risks: A dangerous regulatory paradox. *Applied Stochastic Models in Business and Industry 39*: 549–66.

Carfora, Maria Francesca, Fabio Martinelli, and Francesco Mercaldo. 2019. Cyber risk management: An actuarial point of view. *Journal of Operational Risk* 14: 77–103. [CrossRef]

Cherubini, Umberto. 2024. Multivariate security breach probability: The gordon-loeb model with copulas. Paper presented at International Conference on Computer Safety, Reliability, and Security, Florence, Italy, September 17, pp. 257–65.

Chong, Wing Fung, Daniël Linders, Zhiyu Quan, and Linfeng Zhang. 2025a. Incident-specific cyber insurance. *ASTIN Bulletin: The Journal of the IAA* 55: 395–425. [CrossRef]

Chong, Wing Fung, Runhuan Feng, Hins Hu, and Linfeng Zhang. 2025b. Cyber risk assessment for capital management. *Journal of Risk and Insurance* 92: 424–71. [CrossRef]

Cremer, Frank, Barry Sheehan, Martin Mullins, Michael Fortmann, Stefan Materne, and Finbarr Murphy. 2024. Enhancing cyber insurance strategies: Exploring reinsurance and alternative risk transfer approaches. *Journal of Cybersecurity* 10: tyae027. [CrossRef]

Cremer, Frank, Barry Sheehan, Michael Fortmann, Arash N Kia, Martin Mullins, Finbarr Murphy, and Stefan Materne. 2022. Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance. Issues and Practice* 47: 698. [CrossRef]

Dacorogna, Michel, and Marie Kratz. 2023. Managing cyber risk, a science in the making. *Scandinavian Actuarial Journal* 2023: 1000–21. [CrossRef]

Dacorogna, Michel, Nehla Debbabi, and Marie Kratz. 2023. Building up cyber resilience by better grasping cyber risk via a new algorithm for modelling heavy-tailed data. *European Journal of Operational Research* 311: 708–29. [CrossRef]

Dubois, Thomas, Caner Keskin, and Ufuk Tatar. 2022. Cyber Risk Modeling and Datasets: A Systematic Interdisciplinary Literature Review for Actuaries. Society of Actuaries Research Report. Available online: https://www.soa.org/4a81c2/globalassets/assets/files/resources/research-report/2022/cyber-risk-modeling.pdf (accessed on 2 July 2025).

Dunne, Jonathan, and David Malone. 2017. Obscured by the cloud: A resource allocation framework to model cloud outage events. *Journal of Systems and Software* 131: 218–29. [CrossRef]

Edwards, Benjamin, Steven Hofmeyr, and Stephanie Forrest. 2016. Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity* 2: 3–14. [CrossRef]

Eling, Martin. 2020. Cyber risk research in business and actuarial science. *European Actuarial Journal* 10: 303–33. [CrossRef]

Eling, Martin, and Kwangmin Jung. 2018. Copula approaches for modeling cross-sectional dependence of data breach losses. *Insurance: Mathematics and Economics* 82: 167–80. [CrossRef]

Eling, Martin, and Werner Schnell. 2020. Capital requirements for cyber risk and cyber risk insurance: An analysis of solvency ii, the us risk-based capital standards, and the swiss solvency test. *North American Actuarial Journal* 24: 370–92. [CrossRef]

Eling, Martin, Michael McShane, and Trung Nguyen. 2021. Cyber risk management: History and future research directions. *Risk Management and Insurance Review* 24: 93–125. [CrossRef]

Eling, Martin, Rustam Ibragimov, and Dingchen Ning. 2024. The Changing Landscape of Cyber Risk: An Empirical Analysis of Frequency, Severity, and Tail Dynamics. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5158032 (accessed on 1 July 2025).

European Commission. 2015. *Commission Delegated Regulation (Eu): Supplementing Directive 2009/138/ec of the European Parliament and of the Council on the Taking-Up and Pursuit of the Business of Insurance and Reinsurance (Solvency II)*. Commission Delegated Regulation. Ispra: European Commission.

European Insurance and Occupational Pensions Authority. 2014. The Underlying Assumptions in the Standard Equation for the Solvency Capital Requirement Calculation. EIOPA-14-322. Available online: https://register.eiopa.europa.eu/regulation-supervision/insurance/solvency-ii/solvency-ii-technical-specifications (accessed on 20 June 2025).

European Insurance and Occupational Pensions Authority. 2018. *Understanding Cyber Insurance: A Structured Dialogue with Insurance Companies*. Technical Report. Luxembourg: EIOPA. [CrossRef]

European Insurance and Occupational Pensions Authority. 2019. *Cyber Risk for Insurers: Challenges and Opportunities*. Luxembourg: Publications Office of the European Union. [CrossRef]

European Insurance and Occupational Pensions Authority. 2023. *Methodological Principles of Insurance Stress Testing—Cyber Component*. Technical Report EIOPA(2023)0087508. Frankfurt: EIOPA.

Farkas, Sébastien, Olivier Lopez, and Maud Thomas. 2021. Cyber claim analysis using generalized pareto regression trees with applications to insurance. *Insurance: Mathematics and Economics* 98: 92–105. [CrossRef]

Franke, Ulrik. 2017. The cyber insurance market in sweden. *Computers & Security* 68: 130–44. [CrossRef]

Franke, Ulrik, and Albina Orlando. 2025. Interdependent cyber risk and the role of insurers. *Research in Economics* 79: 101059. [CrossRef]

Gao, Xing, Weijun Zhong, and Shue Mei. 2015. Security investment and information sharing under an alternative security breach probability function. *Information Systems Frontiers* 17: 423–38. [CrossRef]

Georgescu, Tiberiu-Marian. 2021. A study on how the pandemic changed the cybersecurity landscape. *Informatica Economica* 25: 42–60. [CrossRef]

Ghelani, Diptiben. 2022. Cyber security, cyber threats, implications and future perspectives: A review. *Authorea Preprints*. [CrossRef]

Gordon, Lawrence A., and Martin P. Loeb. 2002. The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)* 5: 438–57. [CrossRef]

Gordon, Lawrence A., Martin P. Loeb, and Lei Zhou. 2016. Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security* 7: 49. [CrossRef]

Gordon, Lawrence A., Martin P. Loeb, and Lei Zhou. 2020. Integrating cost–benefit analysis into the nist cybersecurity framework via the gordon–loeb model. *Journal of Cybersecurity* 6: tyaa005. [CrossRef]

Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Lei Zhou. 2014. Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model. *Journal of Information Security* 6: 24. [CrossRef]

Hausken, Kjell. 2006. Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers* 8: 338–49. [CrossRef]

He, Rong, Zhuo Jin, and Johnny Siu-Hang Li. 2024. Modeling and management of cyber risk: A cross-disciplinary review. *Annals of Actuarial Science* 18: 270–309. [CrossRef]

Herath, Hemantha, and Tejaswini Herath. 2007. Cyber-insurance: Copula pricing framework and implication for risk management. In *WEIS*. University Park: Citeseer.

Herath, Hemantha, and Tejaswini Herath. 2011. Copula-based actuarial model for pricing cyber-insurance policies. *Insurance Markets and Companies: Analyses and Actuarial Computations* 2: 7–20.

Huang, C. Derrick, and Ravi S. Behara. 2013. Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. *International Journal of Production Economics* 141: 255–68. [CrossRef]

Kaas, Rob, Marc Goovaerts, Jan Dhaene, and Michel Denuit. 2008. Premium principles and risk measures. *Modern Actuarial Risk Theory: Using R* 115–34.

Kesan, Jay P., Rupterto P. Majuca, and William J. Yurcik. 2004. *The Economic Case for Cyberinsurance*. Technical Report 2. Champaign: University of Illinois College of Law.

Kröger, Wolfgang. 2008. Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering & System Safety* 93: 1781–87. [CrossRef]

Krutilla, Kerry, Alexander Alexeev, Eric Jardine, and David Good. 2021. The benefits and costs of cybersecurity risk reduction: A dynamic extension of the gordon and loeb model. *Risk Analysis* 41: 1795–808. [CrossRef]

Kuper, Gabriel, Fabio Massacci, Woohyun Shim, and Julian Williams. 2020. Who should pay for interdependent risk? policy implications for security interdependence among airports. *Risk Analysis* 40: 1001–19. [CrossRef]

Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason R. C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. 2021. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security* 105: 102248.

Lau, Pikkin, Lingfeng Wang, Zhaoxi Liu, Wei Wei, and Chee-Wooi Ten. 2021. A coalitional cyber-insurance design considering power system reliability and cyber vulnerability. *IEEE Transactions on Power Systems* 36: 5512–24. [CrossRef]

Lau, Pikkin, Wei Wei, Lingfeng Wang, Zhaoxi Liu, and Chee-Wooi Ten. 2020. A cybersecurity insurance model for power system reliability considering optimal defense resource allocation. *IEEE Transactions on Smart Grid* 11: 4403–14. [CrossRef]

Lin, Zhaoxin, Travis Sapp, Rahul Parsa, Jackie Rees Ulmer, and Chengxin Cao. 2018. Pricing cyber security insurance. *Journal of Mathematical Finance* 12. [CrossRef]

Lopez, Olivier, Michel Denuit, Mario Ghossoub, Julien Trufin, Justin Kher, Arthur Maillart, Elisabeth Raes, Hugo Rapior, Mohammed-Amine Skoubani, and Brieuc Spoorenberg. 2025. June. Cyber Risk: Quantification, Stress Scenarios, Mitigation, and Insurance. Available online: https://www.casact.org/article/new-research-offers-breakthrough-cyber-risk-quantification-insurance-industry (accessed on 25 June 2025).

Maglaras, Leandros A., Ki Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras, and Tiago J. Cruz. 2018. Cyber security of critical infrastructures. *ICT Express* 4: 42–45. [CrossRef]

Maillart, Thomas, and Didier Sornette. 2010. Heavy-tailed distribution of cyber-risks. *The European Physical Journal B* 75: 357–64. [CrossRef]

Marotta, Angelica, Fabio Martinelli, Stefano Nanni, Albina Orlando, and Artsiom Yautsiukhin. 2017. Cyber-insurance survey. *Computer Science Review* 24: 35–61. [CrossRef]

Mastroeni, Loretta, Alessandro Mazzoccoli, and Maurizio Naldi. 2019. Service level agreement violations in cloud storage: Insurance and compensation sustainability. *Future Internet* 11: 142. [CrossRef]

Mastroeni, Loretta, Alessandro Mazzoccoli, and Maurizio Naldi. 2022. Pricing cat bonds for cloud service failures. *Journal of Risk and Financial Management* 15: 463. [CrossRef]

Matsuura, Kanta. 2008. Productivity space of information security in an extension of the gordon-loeb's investmentmodel. In *Managing Information Risk and the Economics of Security*. Cham: Springer, pp. 99–119.

Mayadunne, Sanjaya, and Sungjune Park. 2016. An economic model to evaluate information security investment of risk-taking small and medium enterprises. *International Journal of Production Economics* 182: 519–30. [CrossRef]

Mazzoccoli, Alessandro, and Maurizio Naldi. 2020a. Robustness of optimal investment decisions in mixed insurance/investment cyber risk management. *Risk Analysis* 30: 550–64. [CrossRef]

Mazzoccoli, Alessandro, and Maurizio Naldi. 2020b. The expected utility insurance premium principle with fourth-order statistics: Does it make a difference? *Algorithms* 13: 116. [CrossRef]

Mazzoccoli, Alessandro, and Maurizio Naldi. 2021. Optimal investment in cyber-security under cyber insurance for a multi-branch firm. *Risks* 9: 24. [CrossRef]

Mazzoccoli, Alessandro, and Maurizio Naldi. 2022a. An overview of security breach probability models. *Risks* 10: 220. [CrossRef]

Mazzoccoli, Alessandro, and Maurizio Naldi. 2022b. Optimizing cybersecurity investments over time. *Algorithms* 15: 211. [CrossRef]

Mukhopadhyay, Arunabha, Samir Chatterjee, Debashis Saha, Ambuj Mahanti, and Samir K. Sadhukhan. 2013. Cyber-risk decision models: To insure it or not? *Decision Support Systems* 56: 11–26. [CrossRef]

Mukhopadhyay, Arunabha, Samir Chatterjee, Kallol K. Bagchi, Peteer J. Kirs, and Girja K. Shukla. 2019. Cyber risk assessment and mitigation (cram) framework using logit and probit models for cyber insurance. *Information Systems Frontiers* 21: 997–1018. [CrossRef]

Munk, Tine. 2022. *The Rise of Politically Motivated Cyber Attacks: Actors, Attacks and Cybersecurity*. London: Routledge.

Mupa, Munashe Naphtali, Sylvester Tafirenyika, Melody Rudaviro, Tamuka Nyajeka, Mavenge Moyo, and Eliel Kundai Zhuwankinyu. 2025. Machine learning in actuarial science: Enhancing predictive models for insurance risk management. *Iconic Research and Engineering Journals* 8: 493–504.

Naldi, Maurizio, and Alessandro Mazzoccoli. 2018. Computation of the insurance premium for cloud services based on fourth-order statistics. *International Journal of Simulation: Systems, Science and Technology* 19: 1–6. [CrossRef]

Novo, Carolina Cardoso, Mirian Picinini Méxas, and Lidia Angulo Meza. 2025. Applications of cyber insurance in smart cities: A systematic literature review. *International Journal of Information Security* 24: 93. [CrossRef]

Olivieri, Annamaria, and Ermanno Pitacco. 2015. *Introduction to Insurance Mathematics: Technical and Financial Features of Risk Transfers*. Cham: Springer.

Organisation for Economic Co-Operation and Development. 2017. *Enhancing the Role of Insurance in Cyber Risk Management*. Technical Report. Paris: OECD.

Organisation for Economic Co-Operation and Development. 2020. *Encouraging Clarity in Cyber Insurance Coverage. The Role of Public Policy and Regulation*. Technical Report. Paris: OECD.

Pal, Ranjan, Konnie Duan, and Rohan Sequeira. 2025. A theory to estimate, bound, and manage systemic cyber-risk. Paper presented at the 39th ACM SIGSIM Conference on Principles of Advanced Discrete Simulation, Santa Fe, NM, USA, June 23–26, pp. 70–80. [CrossRef]

Pal, Ranjan, Leana Golubchik, Konstantinos Psounis, and Pan Hui. 2014. Will cyber-insurance improve network security? A market analysis. Paper presented at the INFOCOM, 2014 Proceedings IEEE, Toronto, ON, Canada, April 27–May 2, pp. 235–43.

Palsson, Kjartan, Steinn Gudmundsson, and Sachin Shetty. 2020. Analysis of the impact of cyber events for cyber insurance. *The Geneva Papers on Risk and Insurance-Issues and Practice* 45: 564–79. [CrossRef]

Peng, Chen, Maochao Xu, Shouhuai Xu, and Taizhong Hu. 2018. Modeling multivariate cybersecurity risks. *Journal of Applied Statistics* 45: 2718–40. [CrossRef]

Peters, Gareth, Pavel V. Shevchenko, Ruben D. Cohen, and Diane Maurice. 2017. Statistical Machine Learning Analysis of Cyber Risk Data: Event Case Studies. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3200155 (accessed on 18 June 2025).

Pollmeier, Santiago, Ivano Bongiovanni, and Sergeja Slapničar. 2023. Designing a financial quantification model for cyber risk: A case study in a bank. *Safety Science* 159: 106022. [CrossRef]

Rabitti, Giovanni, Amir Khorrami Chokami, Patrick Coyle, and Ruben D Cohen. 2025. A taxonomy of cyber risk taxonomies. *Risk Analysis* 45: 376–86. [CrossRef]

Rangu, Călin Mihail, Leonardo Badea, Mircea Constantin Scheau, Larisa Găbudeanu, Iulian Panait, and Valentin Radu. 2024. Cyber insurance risk analysis framework considerations. *The Journal of Risk Finance* 25: 224–52. [CrossRef]

Ratnawat, Chetan Prakash. 2025. Revolutionizing cyber insurance: Ai-driven risk scorecards for smes. *Journal Of Multidisciplinary* 5: 27–37. [CrossRef]

Romanosky, Sasha, Lilian Ablon, Andreas Kuehn, and Therese Jones. 2019. Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk? *Journal of Cybersecurity* 5: tyz002. [CrossRef]

Shetty, Nikhil, Galina Schwartz, Mark Felegyhazi, and Jean Walrand. 2010. Competitive cyber-insurance and internet security. In *Economics of Information Security and Privacy*. Cham: Springer, pp. 229–47. [CrossRef]

Skeoch, Henry R. K. 2022. Expanding the gordon-loeb model to cyber-insurance. *Computers & Security* 112: 102533. [CrossRef]

Smith, Zhanna Malekos, and Eugenia Lostri. 2020. *The Hidden Costs of Cybercrime*. Technical Report. Santa Clara: McAfee.

Sobchuk, Valentyn, Oleg Barabash, Andrii Musienko, Iryna Tsyganivska, and Oleksandr Kurylko. 2023. Mathematical model of cyber risks management based on the expansion of piecewise continuous analytical approximation functions of cyber attacks in the fourier series. *Axioms* 12: 924. [CrossRef]

Strupczewski, Grzegorz. 2019. What is the worst scenario? modeling extreme cyber losses. Paper presented at the Multiple Perspectives in Risk and Risk Management: ERRN 8th European Risk Conference 2018, Katowice, Poland, September 20–21. Cham: Springer, pp. 211–30.

Strzelczyk, Wojciech, and Karolina Puławska. 2025. Unraveling the role of cyber insurance in fortifying organizational cybersecurity. *MIS Quarterly Executive* 24: 35–45. [CrossRef]

Sun, Hong, Maochao Xu, and Peng Zhao. 2021. Modeling malicious hacking data breach risks. *North American Actuarial Journal* 25: 484–502. [CrossRef]

Taherdoost, Hamed. 2022. Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. *Electronics* 11: 2181. [CrossRef]

Tsohou, Aggeliki, Vasiliki Diamantopoulou, Stefanos Gritzalis, and Costas Lambrinoudakis. 2023. Cyber insurance: State of the art, trends and future directions. *International Journal of Information Security* 22: 737–48. [CrossRef]

Venkatachary, Sampath Kumar, Jagdish Prasad, and Ravi Samikannu. 2017. Economic impacts of cyber security in energy sector: A review. *International Journal of Energy Economics and Policy* 7: 250–62.

Wang, Shaun. 2017. Optimal Level and Allocation of Cybersecurity Spending: Model and Formula. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3010029 (accessed on 10 June 2025).

Wang, Shaun S. 2019. Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal* 57: 101173. [CrossRef]

Weber, Stefan, Matthias Scherer, Corina Pascu, and Marco Barros Lourenco. 2024. *Cyber Insurance—Models and Methods and the Use of AI*. Technical Report. Athens: European Union Agency for Cybersecurity. [CrossRef]

Weisman, Michael J., Alexander Kott, Jason E. Ellis, Brian J. Murphy, Travis W. Parker, Sidney Smith, and Joachim Vandekerckhove. 2025. Quantitative measurement of cyber resilience: Modeling and experimentation. *ACM Transactions on Cyber-Physical Systems* 9: 1–25. [CrossRef]

Wheatley, Spencer, Thomas Maillart, and Didier Sornette. 2016. The extreme risk of personal data breaches and the erosion of privacy. *The European Physical Journal B* 89: 1–12. [CrossRef]

Woods, Daniel W., and Josephine Wolff. 2025. A history of cyber risk transfer. *Journal of Cybersecurity* 11: tyae028. [CrossRef]

Xiang, Qikun, Ariel Neufeld, Gareth W Peters, Ido Nevat, and Anwitaman Datta. 2024. A bonus-malus framework for cyber risk insurance and optimal cybersecurity provisioning. *European Actuarial Journal* 14: 581–621. [CrossRef]

Xu, Lu, Yanhui Li, and Jing Fu. 2019. Cybersecurity investment allocation for a multi-branch firm: Modeling and optimization. *Mathematics* 7: 587. [CrossRef]

Xu, Maochao, and Lei Hua. 2019. Cybersecurity insurance: Modeling and pricing. *North American Actuarial Journal* 23: 220–49. [CrossRef]

Xu, Maochao, Kristin M. Schweitzer, Raymond M. Bateman, and Shouhuai Xu. 2018. Modeling and predicting cyber hacking breaches. *IEEE Transactions on Information Forensics and Security 13*: 2856–71.

Yang, Zichao, and John CS Lui. 2014. Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Performance Evaluation* 74: 1–17. [CrossRef]

Young, Derek, Juan Lopez, Mason Rice, Benjamin Ramsey, and Robert McTasney. 2016. A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection* 14: 43–57. [CrossRef]

Zängerle, Daniel, and Dirk Schiereck. 2023. Modelling and predicting enterprise-level cyber risks in the context of sparse data availability. *The Geneva Papers on Risk and Insurance-Issues and Practice* 48: 434–62. [CrossRef]

Zeller, Gabriela, and Matthias Scherer. 2022. A comprehensive model for cyber risk based on marked point processes and its application to insurance. *European Actuarial Journal* 12: 33–85. [CrossRef]

Zraqou, Jamal, Khalil Omar, and Jawad H. Alkhateeb. 2025. The evolution of cyber insurance in response to artificial intelligence risks. In *Cybersecurity Insurance Frameworks and Innovations in the AI Era*. Hershey: IGI Global. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.