

# Cyber Risk Modeling Methods and Data Sets: A Systematic Interdisciplinary Literature Review for Actuaries

September | 2022



# Cyber Risk Modeling Methods and Data Sets

A Systematic Interdisciplinary Literature Review for Actuaries

**AUTHORS** Elisabeth V. Dubois, MBA

Omer F. Keskin, Ph.D.

Unal Tatar, Ph.D.

**SPONSOR** General Insurance Research Committee  
of the Society of Actuaries Research  
Institute



**Give us your feedback!**

Take a short survey on this report.

[Click Here](#)



#### **Caveat and Disclaimer**

The opinions expressed and conclusions reached by the authors are their own and do not represent any official position or opinion of the Society of Actuaries Research Institute, the Society of Actuaries or its members. The Society of Actuaries Research Institute makes no representation or warranty to the accuracy of the information.

Copyright © 2022 by the Society of Actuaries Research Institute. All rights reserved.

## CONTENTS

<b>Executive Summary .....</b>	<b>5</b>
<b>Nomenclature .....</b>	<b>7</b>
<b>Section 1: Introduction .....</b>	<b>8</b>
<b>Section 2: Methodology .....</b>	<b>12</b>
2.1 Protocol .....	12
2.2 Eligibility Criteria .....	12
2.3 Search Strategy .....	13
2.4 Academic Review Method .....	14
2.5 Grey Literature Review Method .....	14
2.6 Validation .....	15
2.7 Limitations .....	15
2.8 Project Risks & Mitigation .....	15
<b>Section 3: Bibliometrics Analysis of Academic Studies .....</b>	<b>16</b>
<b>Section 4: Modeling &amp; Pricing Methods .....</b>	<b>21</b>
4.1 Non-Systemic Risks vs. Systemic vs. Operational Risks .....	21
4.2 Methods .....	22
4.2.1 Traditional Actuarial Theory and Practice .....	22
4.2.2 Simulations .....	23
4.2.3 Game Theory .....	25
4.2.4 Network Models .....	28
4.2.5 Case Study .....	30
4.2.6 Statistical Analysis .....	33
4.2.7 Non-Intrusive Risk Scoring .....	37
4.2.8 AI & Machine Learning .....	38
<b>Section 5: Datasets for Cyber Risk Modeling and Quantification .....</b>	<b>40</b>
5.1 Datasets used by Actuarial and Insurance Research .....	40
5.1.1 Chronology of Data Breaches provided by the Privacy Rights Clearinghouse (PRC) .....	41
5.1.2 SAS® OpRisk Global Data .....	42
5.1.3 SERFF filings from NAIC .....	42
5.1.4 ISTR Report from Symantec .....	42
5.1.5 Thomas Reuters Eikon .....	42
5.1.6 Advisen’s Cyber Database .....	43
5.1.7 Cowbell Cyber Inc. Cyber Data .....	43
5.1.8 Private/Proprietary Datasets .....	43
5.2 Additional Cyber-Risk-Related Datasets .....	44
5.2.1 Cyber AcuView .....	44
5.2.2 DataLossDB .....	44
5.2.3 DHS Impact .....	44
5.2.4 NetDiligence .....	45
5.2.5 FBI Internet Crime Complaint Center Report .....	45
5.2.6 ISO Verisk .....	45
5.2.6 ORX Operational Risk Data .....	45
5.2.7 PONEMON Institute Cost of Data Breach Study .....	45
5.2.8 VERIS Community Database (VCDB) .....	45
5.2.9 Common Vulnerabilities and Exposures (CVE) .....	46
5.2.10 Common Vulnerability Scoring System (CVSS) .....	46
5.2.11 Honeypot Data .....	46
<b>Section 6: Challenges .....</b>	<b>47</b>

6.1 Inadequate Data .....	47
6.2 Information Asymmetry .....	47
6.3 Correlated and Interdependent Risks.....	47
6.4 Quantification of Cyber Risk.....	48
<b>Section 7: Knowledge Gaps &amp; Future Research .....</b>	<b>49</b>
<b>Section 8: Acknowledgments .....</b>	<b>52</b>
<b>Appendices .....</b>	<b>53</b>
Appendix A: Google Scholar Citations.....	53
Appendix B: Compendium of Grey Literature .....	54
Appendix C: Compendium of Academic Literature.....	60
Appendix D: Compendium of Cyber Insurance Datasets.....	71
<b>References – Grey Literature.....</b>	<b>73</b>
<b>References – Academic Literature.....</b>	<b>80</b>
<b>References – Other .....</b>	<b>87</b>
<b>About The Society of Actuaries Research Institute .....</b>	<b>90</b>

# Cyber Risk Modeling & Datasets: A Systematic Interdisciplinary Literature Review for Actuaries


## Executive Summary

With increasing cyber threats, both practitioners and academics have sought ways to address them, one of which is via cyber insurance. Despite the increasing importance of such work for businesses and society, research on cyber insurance is limited. Most of the research that exists is published in computer science, with limited research in the fields of business and actuarial science, although studies are beginning to delve into these fields. Existing research highlights the lack of data and modeling challenges and the difficulties and complexities of measuring risks. Furthermore, an additional problem in the field is that the research is scattered among the communities of cybersecurity experts. Practitioners from the insurance and actuarial sector require these research endeavors to be gathered, analyzed, and synthesized to be able to benchmark the existing methods and apply them to their business. Such a requirement can be achieved by a comprehensive literature search that presents the existing cyber risk analysis methods and the gaps in the literature for further improvement.

This report reviews the academic and grey literature on “cyber insurance” and “cyber actuary” across multiple disciplines. Grey literature includes a wide range of resources produced outside of traditional publishing and distributing channels, such as reports by government agencies, non-governmental organizations, and companies. The results of the literature review that includes academic and grey literature correspond to the notion that cyber risk is an increasingly important research topic that has grown exponentially in many disciplines (see Appendix A), but limited attention to date has been given to actuarial science. Using the PRISMA review method, the study collects and analyzes over 200 studies, reports, etc. from a variety of academic and grey literature sources. The literature is categorized in a compendium that filters the articles based on the presence of data, methodologies used, and modeling techniques. Next, the data extracted is systematically mapped to highlight the challenges and knowledge gaps in cyber actuarial research and share future research directions for academics and practitioners.


The results of the study can be grouped thematically to provide an overview of the literature for researchers and practitioners in cyber risk, insurance, and actuaries. The first group of the literature is comprised of studies that develop new models, approaches, or datasets for cyber risk quantification and modeling. The second group consists of studies that adopt a current cyber risk quantification method on a new domain. The third group provides a summary of findings of previous research or the status of the cyber insurance market. Additionally, this study reviewed the various challenges that actuaries and cyber insurers face when quantifying cyber risks.

The implications of this study are far-reaching for both practitioners and academics. This study contributes to the current body of literature by being the most extensive review to date that incorporates both academic and grey literature. Likewise, the study will provide academics and practitioners with a comprehensive, interdisciplinary synopsis of the methods, datasets, challenges, and future directions that will aid actuaries and risk managers.



**Give us your feedback!**  
Take a short survey on this report.

[Click Here](#)



## Nomenclature

CAS	Casualty Actuarial Society
CIA	Canadian Institute of Actuaries
CIPR	The Center for Insurance Policy and Research of NAIC
CISA	Cybersecurity and Infrastructure Security Agency
CRISM	Cyber Risk Scoring and Mitigation
CSRC	Computer Security Resource Center
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DHS	U.S. Department of Homeland Security
ENISA	European Network and Information Security Agency
EIOPA	European Insurance and Occupational Pensions Authority
FBI	Federal Bureau of Investigation
FTC	Federal Trade Commission
GAO	U.S. Government Accountability Office
IC3	Internet Crime Complaint Center
IMPACT	Information Marketplace for Policy and Analysis of Cyber Risk and Trust
IoT	Internet of Things
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISTR	Internet Security Threat Report
NAIC	National Association of Insurance Commissioners
NIST	National Institute of Standards and Technology
OECD	Organization for Economic Co-operation and Development
PII	Personally Identifiable Information
PRC	Privacy Rights Clearinghouse
PRISMA	Preferred Reporting Items for Systematic reviews and Meta-Analyses
RUSI	Royal United Services Institute for Defence and Security Studies
SOA	Society of Actuaries
VCDB	VERIS Community Database

## Section 1: Introduction

Cyber risks present a major threat to individuals, businesses, and governments worldwide. In recent years, the cost of cyber-crimes has increased exponentially – from \$3 trillion annually in 2015 to an estimated \$10.5 trillion annually by 2025 (Morgan, 2020). As the cost of cybercrime continues to expand, many are looking to transfer their risk to insurance companies or third parties. Stakeholders have various roles and responsibilities to improve the cyber insurance market (Cybersecurity and Infrastructure Security Agency [CISA], 2012). CISA (2013, 2014b) outlined four “pillars” of an effective cyber risk culture that insurers had identified as attractive from an underwriting perspective: “engaged executive leadership; targeted cyber risk education and awareness; cost-effective technology investments; and relevant information sharing.” According to a market convergence report (Aite Novarica, 2016), the cyber insurance market was still considered in its infancy in 2016, with the insurers' attempts to shield from silent cyber exposure. Silent cyber causes confusion for the insureds and conflicts regarding claims for insurers since losses regarding emerging cyber risks are not explicitly included or excluded, and the language of the policy is ambiguous or conflicting (Bean, 2020; Cambridge Centre for Risk Studies, 2017; Carter et al., 2020; Dale, 2020; Lloyd’s, 2020b; Marsh, 2020b; 2020c; Marsh McLennan, 2020; OECD, 2020a; Tatar et al., 2021). The clarity in cyber insurance coverage is encouraged to overcome this issue, leading to more effective cyber insurance coverage for both parties and a more sustainable insurance market (Cowbell Cyber, 2022; U.S. Government Accountability Office [GAO], 2021; Wolfram, 2020).

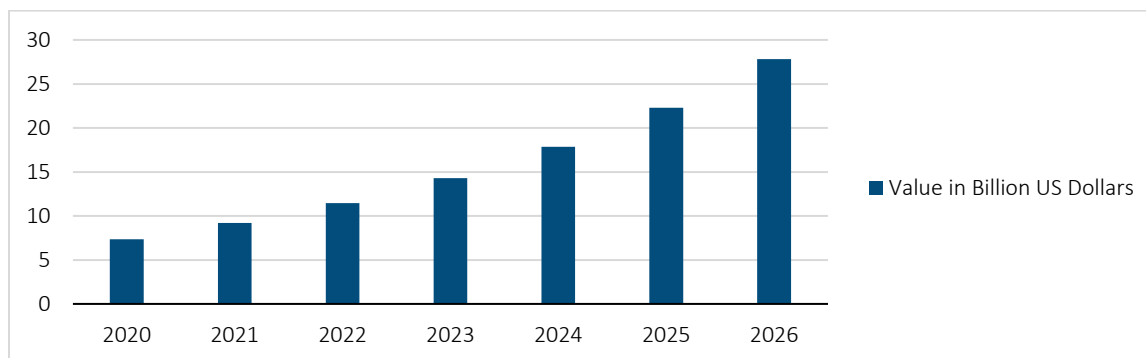
GAO (2021) identified key trends in the current cyber market as increased prices, increased take-up rate (i.e., the proportion of existing insureds electing new coverage in cyber), and lowered limits on cyber insurance policies due to the increased attack severity. The high inconsistency in the pricing for the same amount of coverage in 2015 was indicated by the Organization for Economic Co-operation and Development (OECD) (OECD, 2017) as up to 600% variation among different insurers. However, there has been an improvement in the market consistency; a survey that Advisen and PartnerRe conducted in 2020 with 260 cyber insurance brokers and 190 cyber insurers reported increased market consistency in cyber insurance pricing (61%) and coverage (72%). The reasons behind the increased consistency were determined as the use of risk modeling and more experience in cyber risks. Other surveys and reports indicated increased pricing and tougher underwriting as the changes in the cyber insurance market (Advisen and Zurich, 2020; Aon, 2021; Carter et al., 2020; European Insurance and Occupational Pensions Authority [EIOPA], 2020; Gallagher Re & Risk Management Solutions, Inc., 2022; Hartwig and Wilkinson, 2015; Howden, 2021; Johansmeyer, 2021; Marsh, 2020, 2022; OECD, 2017; Reagan et al., 2020; World Economic Forum, 2022). Although prices increase, the demand for cyber risk coverage also increases, primarily due to the changing exposure environment, internal risk analysis of insureds, and broker recommendations (Advisen and Zurich, 2020; NAIC, 2021; OECD, 2018). It is estimated that the global cyber insurance market will expand by 25% per year, reaching almost \$28 billion by 2026 (see Figure 1).

Nevertheless, the ever-changing risk landscape, including sophisticated ransomware, attacks on the digital supply chain, and deep vulnerabilities, have exposed severe technology gaps presenting increased challenges for actuaries (Moore, 2022). According to the trends of recent claims for cyber insurance coverage, the most common cyber incidents are ransomware, funds transfer fraud, and email compromise, while most claims cover breach response costs, cyber extortion liabilities (ransom payment), and funds transfer fraud that is caused by social engineering attacks (Coalition, 2021; Corax & Clyde&Co, 2018; NetDiligence, 2021; Willis Tower Watson, 2020). Due to the rise in attack sophistication, increases in losses, and increases in entities that took out cyber insurance, insurers faced the “perfect storm,” resulting in significant losses (Adamczyk, 2022). In the short term, many insurers raised their premiums to compensate for the cost of the attacks but realize that in the long-term, they will have to look for improved ways to calculate cyber risk, model premiums, and help customers mitigate their cyber risk (European Network and Information Security Agency [ENISA], 2016). This also raises concerns regarding the



substantial costs that systemic cyber risks can cause for insurers. A recent report from GAO (2022) recommended the assessment of the government's potential involvement to cover the losses of catastrophic cyber incidents against the critical infrastructure sector due to insurers' reluctance regarding systemic cyber incidents.

**Figure 1**  
**GLOBAL CYBER INSURANCE MARKET GROWTH**



Adapted from (Rudden, 2022)

Although cyber-attacks are a regular occurrence, many attacks in recent years exemplify the impact and severity of cyber threats. In 2016, nation-state actors sought to interfere with U.S. elections by hacking the Democratic National Committee and accordingly interfering with the democratic process (FBI, 2018). In 2017, the WannaCry ransomware attack managed to affect more than 200,000 Windows computers in 150 countries, holding several critical infrastructure systems hostages, including the United Kingdom's National Health Service Hospitals (Department of Health, 2018). Similarly, in 2017, cyber threat actors hacked Equifax, stealing over 145 million sensitive records, including Personally Identifiable Information (PII) (Federal Trade Commission [FTC], 2017). In 2020, a digital supply chain attack initially infected computer systems of SolarWinds (which provides IT management software and services to businesses and government agencies) and spread to their customers, in one of the largest and most sophisticated cyber operations, affecting the confidentiality and availability of several federal agencies, courts, private companies, and state and local governments and eventually caused widespread economic damage (Blunt, 2021). In 2021, Colonial Pipeline paid a \$4.4 million ransom to put their systems back online after their fuel pipeline was taken down due to one compromised password, leading to gas shortages and subsequent increase in gas prices across the East Coast (Office of Cybersecurity, Energy Security, and Emergency Response, 2021). These examples further emphasize the far-reaching impact of cyber-attacks and the increasing risks in cyberspace, where sophisticated threat actors can penetrate the most secure systems and cause consequential disruption, personal harm, and financial damage. As highlighted, cyber-attacks can spread across systems, causing outages or system breaches across sectors (Cambridge Centre for Risk Studies, 2018).

According to the Computer Security Resource Center (CSRC) under NIST (2022), cyber risk is defined as "the risk of depending on cyber resources (i.e., the risk of depending on a system or system elements that exist in or intermittently have a presence in cyberspace)." The term cyber risk itself encompasses various types of risks that have different causes and impacts on systems or entities. Cyber risks include email or Internet fraud, identity fraud, theft of financial, health, or personally identifiable information (PII), theft or sale of PII or corporate data, ransomware, cyber extortion, crypto-jacking, cyberespionage, and more. Today's cyber risks often lead to loss of confidentiality, integrity, and availability (CIA) of data and services, increasing the risk to the entity infected, the public, and the insurer. In this, cybercrimes have many hidden costs, including opportunity costs, time and money spent on cybersecurity decision-making, system downtime,

loss of productivity, stolen intellectual property (Lloyd's, 2020b), and reputational damage, whereupon many of these costs are not easy to quantify (Smith et al., 2020).

Therefore, cyber risk has been a critical issue for the insurance industry for several years but from two quite different perspectives. The first is from the product design/pricing and managing insurance risk exposure. The second perspective is addressing the operational risks that confront insurers. As cyber threats grow, so does the market for cyber insurance to mitigate the risk, yet cyber risks have to be understood from an actuarial viewpoint, and cyber insurers and insureds need to be equipped to adjust to the non-stationary cyber landscape.

Another aspect of cyber insurance is that it is considered to have the potential to govern cybersecurity and incentivize the improvement of cybersecurity hygiene. Woods and Moore (2020) suggest that the evidence in the market does not support this concept; rather, cyber insurance only marginally incentivizes the insureds to improve their cybersecurity posture. The policymakers instead focus more on covering the post-incident third-party recovery costs, possibly due to making their policy more manageable. Cyber insurance in its current form is more perceived as a cyber resilience tool rather than risk mitigation (MacColl et al., 2021). Especially small and medium-sized enterprises can benefit from cyber insurance as a cyber resilience means (Hoffman, 2016) since there is a considerable chance that they cannot survive a high-impact cyber-attack. Although OECD (2017) suggests that insurance can improve the cybersecurity of companies and countries, the findings of Sullivan and Nurse (2020) suggest that the improvement of cybersecurity posture using cyber insurance is still only in the theoretical phase; moreover, many customers are skeptical about the benefits of cyber insurance.

Increasing cyber incidents and emergent characteristics of cyber threats have led researchers and practitioners to produce innovative approaches to address them. Moreover, the lack of data obstructs the utilization of traditional actuarial methods, leading government agencies to encourage researchers to build datasets and share information (CISA, 2014b; 2014c; Coburn et al., 2018). That is why subject matter experts from academia, industry, and sometimes the government have developed new methods. New datasets also have emerged to address the lack of historical data in cybersecurity. However, only larger firms have the resources to build relevant actuarial models for these datasets (Corix Partners & Cyber Solace, 2022). Despite the increasing importance of such work for businesses and society, research on cyber insurance is limited. Most of the research that exists is published in computer science, with limited research in the fields of business and actuarial science, although studies are beginning to delve into these fields. Existing research highlights the lack of data and modeling challenges and the difficulties and complexities of measuring risks. Furthermore, an additional problem in the field is that the research in the literature is scattered across the communities of cybersecurity experts. Researchers and practitioners are working towards putting a price on cyber risks and will continue this effort for the following few years (Aon, 2021). In this manner, establishing a public-private partnership to develop new models in cyber insurance pricing is deemed necessary (U.S. Cyberspace Solarium Commission, 2020).

Cyber insurance policy pricing is “not one size fits all” since premiums are calculated based on a company’s size, sector, historical loss experience, risks and exposures, business processes, provided coverage, customers’ behavior, jurisdiction, policy limits, type of sensitive data handled, number of records, level of encryption, network security practices, information security policies, annual gross revenue and other factors using various methods (EIOPA, 2018; Marciano, 2020). Due to the lack of quality data, most companies use qualitative models, such as pricing tools that leverage risk assumptions of exposure, rating approach that leverage questionnaires, or expert judgment. Although quantitative approaches, such as actuarial pricing rating tools and ensemble models that employ various parameters (EIOPA, 2018), exist, the lack of methodology is still considered a significant challenge in the cyber insurance market (CISA, 2019).

Practitioners from the insurance and actuarial sector require the current research endeavors about modeling and pricing to be gathered, analyzed, and synthesized to be able to benchmark the existing methods and apply the suitable ones to their businesses. Such a requirement can be achieved by a comprehensive literature search that presents the existing cyber risk analysis methods and the gaps in the literature for further improvement.

The purpose of this project is to conduct a literature search regarding the existing cyber risk analysis methods and gaps in the cyber risk field. To accomplish this purpose, the authors conducted a PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) review (Page et al., 2021) of the academic and grey literature on “cyber insurance” and “cyber actuary” across multiple disciplines. The results correspond to the notion that cyber risk is an increasingly important research topic that has grown exponentially in many disciplines (see Appendix A), but limited attention to date has been given to actuarial science. We define the following research questions based on the research objectives:

*Research Question 1:* What methods are developed to assess cyber risks?

*Research Question 2:* What are the available datasets for cyber risk assessment?

*Research Question 3:* What are the challenges in cyber risk literature for actuaries?

*Research Question 4:* What are the knowledge gaps and future research directions in cyber risk research for actuaries?

To our knowledge, this review contributes to practitioners and academics serving as the most comprehensive to date. The most comparable study is by Eling (2020), who reviewed academic literature on cyber risk and cyber insurance in the fields of business and actuarial science by searching the Web of Science. Although they reviewed business research and actuarial science research, their study sought to only understand the modeling methods used by the academic studies they collected. Awiszus et al. (2021) survey academic literature on modeling and pricing cyber insurance, but they do not provide a clear methodology on the sources utilized or papers searched. Similarly, Marotta et al. (2017) survey academic literature on the main approaches and techniques related to risk management to understand cyber insurance development, modeling, and future directions; yet again, no review methodology is presented. Also, Eling and Schnell (2016) and the Cyber Risk Insurance Task Force and the American Academy of Actuaries Casualty Practice Council (2019) provided lists of resources relevant to cyber insurance. Our study can be differentiated from prior studies in several facets, including the expansive scope without time restrictions, review of several sources across disciplines, and inclusion of grey literature. Unlike prior research, our scope entails reviewing academic and grey literature using a variation of the search terms cyber, actuary, and insurance across all fields, including interdisciplinary work. Within this, we searched all major databases (IEEE Explore, ACM, Springer, Science Direct, Web of Science), 17 of the most commonly referenced insurance and actuarial journals, and grey literature with no time restrictions. In searching for studies on insurance or actuarial modeling, pricing, and/or data sources, we found 100 academic studies as well as 99 grey literature.

The remainder of this report is structured as follows. Section 2 presents the methodology used for this research. Section 3 provides a high-level analysis of the literature. Section 4 presents the modeling and pricing methods used to study cyber insurance. In the following section, Section 5, we evaluate and discuss the datasets used and highlight other publicly available cyber datasets that could be used. Section 6 discusses the challenges in modeling and pricing cyber insurance. In Section 7, we highlight the knowledge gaps identified and future directions for research.

## Section 2: Methodology

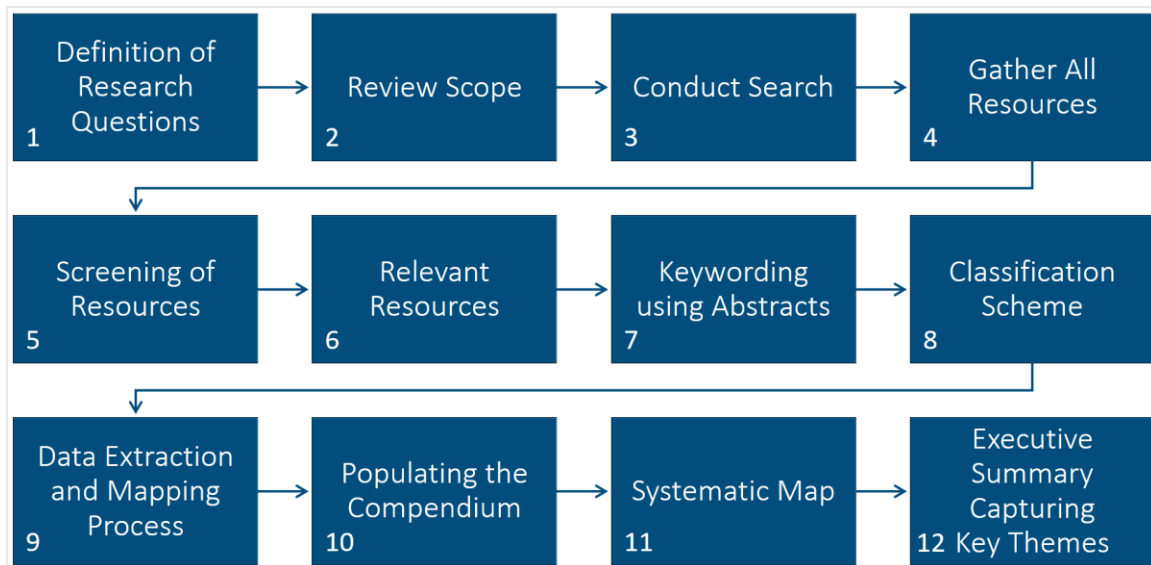
Our primary research methodology was to conduct a systematic literature review, defined as “a review that uses explicit, systematic methods to collate and synthesize findings of studies that address a clearly formulated question” (Page et al., 2021, p. 3) to meet the objectives of this research. We follow the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) method, which “was designed to help systematic reviewers transparently report why the review was done, what the authors did, and what they found” (Page et al., 2021, p. 1). PRISMA is widely used by researchers conducting systematic literature reviews to convey the advancements “reflects advances in methods to identify, select, appraise, and synthesize studies.”

### 2.1 PROTOCOL

We utilized the checklist of the PRISMA method that provides details for reporting and provides a framework for collecting information from each resource (Page et al., 2021). One advantage of the checklist is that it establishes a well-defined structure that eases further extension of the study in the future by analyzing new resources. The PRISMA method and its checklist are used as a standard to result in high-quality systematic literature reviews by prominent academic venues.

The results of the systematic literature review help us map existing research areas and identify gaps that reveal potential research directions. The process we follow is presented in Figure 2. During the duration of the project, Steps 3-6 were repeated regularly to ensure the reported research was as up to date as possible.

**Figure 2**  
THE SYSTEMATIC LITERATURE REVIEW PROCESS



### 2.2 ELIGIBILITY CRITERIA

**Type of Studies** – The search is conducted from sources that include but are not limited to commonly referenced databases, journals, actuarial societies, companies, and government publications. Within this, all major academic databases, including IEEE Explore, ACM, Springer, Science Direct, and Web of Science, are explored. These databases cover academic journals from management, economics, finance, engineering, and other fields. Academic journals from risk management, actuarial, and insurance fields are

also reviewed, including but not limited to *Annals of Actuarial Science*, *ASTIN Bulletin*, *British Actuarial Journal*, *European Actuarial Journal*, *Insurance: Mathematics and Economics*, *North American Actuarial Journal*, *Scandinavian Actuarial Journal*, *South African Actuarial Journal*, and the *Geneva Papers on Risk and Insurance*. Books and book chapters, as well as conference proceedings, were referenced as well. To ensure comprehensive results, we also included publications from actuarial societies (i.e., SOA, CAS, and CIA), publications of insurance companies, and publications of companies that provide modeling or data services to the insurance companies (i.e., Verisk, BitSight, and SecurityScorecard), databases/datasets created to address relevant cyber risk problems, and government publications, including reports, analyses, and recommendations.

**Study Design** – We included conceptual and empirical studies as well as grey literature. Grey literature was not included in the existing literature surveys since they are usually deemed inferior in quality compared to peer-reviewed studies. However, developments in cyber risk literature are emerging, and grey literature includes innovative methods that have not yet been published in academic journals or books. Therefore, in this study, we also include high-quality studies existing in grey literature. Examples of grey literature include conference abstracts, presentations, proceedings; regulatory data; unpublished trial data; government publications; reports (such as white papers, working papers, and internal documentation); dissertations/theses; patents; and policies & procedures (Cantrell, 2022). Review articles were included as they provide insight and points of reference for this review.

**Topic** – We are interested in records that discuss insuring cyber systems. In this, we include articles that provide insurance models or data sources applicable to cyber, methods used to address cyber risks from the insurers' perspective, cyber insurance pricing, those that discuss the cost of cyber incidents, and challenges, solutions, or future directions of cyber risks.

**Language** – We only select English written records per common practice, given the difficulties in translating and reproducing the review (Page et al., 2021).

### 2.3 SEARCH STRATEGY

The relevant research was searched within the academic databases and in grey literature because of the interdisciplinary characteristics of this field. "Grey literature stands for manifold document types produced on all levels of government, academics, business and industry in print and electronic formats [...], but not controlled by commercial publishers" (Schopf, 2010). All major relevant databases and grey literature were queried based on the identified keywords. The results of the search queries are manually analyzed to remove duplicates and irrelevant articles. This was followed by a thorough analysis of each article to identify the practices and challenges within the cyber insurance sector.

First, on January 20, 2022, we searched using a combination of the words cyber, insurance, and actuaries in each of the selected databases. From there, articles were included in Stage 1 if the combination of the search terms were in the title, keywords, abstract, or corresponding metadata. First, Web of Science was searched where 355 records were found searching Topic (i.e., title, abstract, and keywords). Next, IEEE was searched, resulting in 226 records searching All Metadata (i.e., title, abstract, and keywords). In searching ACM, a total of 27 unique records were found searching Title, Abstract, and Keywords separately. Since Springer Link only allows for full-text and title searches, we searched the keywords in full-text records, resulting in 453 records. Seeing as we only wanted records that contained the keywords in the title, abstract, or keywords, we manually searched each aspect in the 453 records and removed 397 records that did not include the keywords in the titles, abstracts, or keywords. At this point, records whose titles or abstracts were not in English (many were in German) or those records that were full-conference proceedings or abstracts were removed, resulting in 67 records from Springer Link. Lastly, for database

searches, we searched the keywords in Science Direct, resulting in 56 records. Following the initial database searches, duplicate articles were merged, and a total of 537 non-duplicate results remained.

To ensure a comprehensive review was conducted on February 9, 2022, we also searched 17 commonly referenced insurance or actuarial journals using search terms including cyber and other synonyms of cyber. The journals searched include Tort Trial and Insurance Practice Law Journal (7 records), The Geneva Risk and Insurance Review (2 records), Geneva Papers on Risk and Insurance: Issues and Practices (41 records), Risk Management and Insurance Review (18 records), Insurance: Mathematics and Economics (11 records), ASTIN Bulletin (11 records), Variance (1 record), Annals of Actuarial Science (8 records), Journal of Risk (0 records), Journal of Risk and Insurance (5 records), Journal of Risk & Uncertainty (1 record), Risk Management (6 records), North American Actuarial Journal (8 records), European Actuarial Journal (4 records), Scandinavian Actuarial Journal (2 records), British Actuarial Journal (25 records), and the South African Actuarial Journal (0 records). All 150 relevant records were included in Stage 1 of this review. In total, 687 records proceeded to Stage 2.

## 2.4 ACADEMIC REVIEW METHOD

Next, all the authors independently screened the titles and abstracts of the 560 articles found via the database searches. Using the exclusion criteria listed below, we removed 355 articles that did not meet one or more of the set criteria based on the abstracts and titles. After removing the 357 articles, 203 remained for full-text review.

Third, we screened the full text of the remaining 203 articles and removed any duplicates that were found when merging the database and journal results. We eliminated 91 articles using the same exclusion criteria as above. To ensure a comprehensive review of all of the literature published to date on this topic, we conducted additional searches in select databases, and actuarial journals previously searched as well as Google Scholar using the selected keywords from February to May 2022. During these additional searches, we reviewed the abstracts and full text of the new articles, along with the date of publication, to ensure they fit all the eligibility criteria and were not already included in the original literature search. Once completed, 13 articles were added to the final articles.

The full-text screening of academic articles led to the inclusion of 100 academic studies for review in this paper.

## 2.5 GREY LITERATURE REVIEW METHOD

Using the internet search engines, we also searched the grey literature for cyber insurance. Since the search engines provide tens of thousands to millions of results for the keywords relevant to this study, we have identified relevant governmental and private organizations in the cyber insurance industry as the sources of the grey literature. After the resource gathering phase, 143 resources that include reports, case studies, articles, podcasts, and videos were analyzed, and 99 resources were selected to be included in this study based on their relevance. Sources of grey literature materials include:

- DHS U.S. Department of Homeland Security
- CISA Cybersecurity and Infrastructure Security Agency
- U.S. GAO United States Government Accountability Office
- NIST National Institute of Standards and Technology
- Publications Office of the European Union
- ENISA European Network and Information Security Agency
- EIOPA European Insurance and Occupational Pensions Authority

- ISACA Information Systems Audit and Control Association
- European Systemic Risk Board
- OECD Organisation for Economic Co-operation and Development
- NAIC National Association of Insurance Commissioners
- CIPR The Center for Insurance Policy and Research of NAIC
- SOA Society of Actuaries
- CAS Casualty Actuarial Society
- Cyentia Institute Cybersecurity Research Library
- RUSI Royal United Services Institute for Defence and Security Studies
- SANS Institute
- Lloyd's
- Marsh McLennan
- Coalition
- TPRM companies' patents and white papers about risk quantification methodologies
- and other sources

## 2.6 VALIDATION

The report is shared with at two cyber risk insurance experts for review to ensure validity and is revised based on their feedback. The feedback from the project oversight group is also utilized for validation purposes.

## 2.7 LIMITATIONS

The literature survey does not include proprietary tools that are relevant to cyber risk and not publicly available. Some of the tools in this field are developed and actively used for commercial purposes. Since research and development efforts regarding these tools are not public information, they are not included in this literature survey. However, the deliverables of this project are open to expansion enabling new research to be included in the compendium. A limitation of the systematic literature review is publication bias in that research with positive results is more likely to be published, whereas research with negative results takes more time to be published or is less cited. To overcome this limitation, the survey includes multiple well-known scientific databases and grey literature. Therefore, the analysis is sufficiently inclusive (Yli-Huumo et al., 2016).

## 2.8 PROJECT RISKS & MITIGATION

We identified two minor project risks and elaborated risk mitigation strategies to address these risks. The first risk for this project is missing the most recent publications, which are revealed after the identification of records phase of this project. Cyber risk is a quickly changing field that results in many new publications regularly. To mitigate this risk, we queried the databases and other resources listed in Section 2.2 monthly to find out the new papers and reports to include in our final report and other deliverables. Another risk of this project is the multidisciplinary and applied nature of cyber risk. In this field, it is not unusual that non-academic publications can provide a strong method, tool, or dataset. For instance, third-party risk scoring applications provided in the industry are elaborated in white papers or patents instead of peer-reviewed journal publications. In an academic literature survey, these sources can be easily ignored or overlooked. To mitigate this risk, we include grey literature in our search and analyze the relevant works that can help the insurance sector and actuaries.

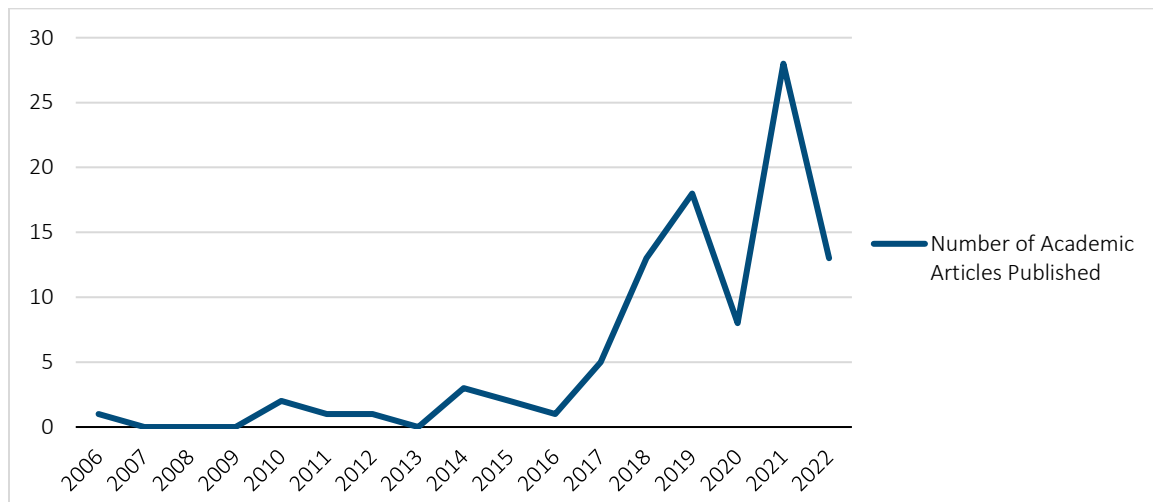
## Section 3: Bibliometrics Analysis of Academic Studies

Upon completing the analysis of the 100 academic articles, we summarized several study characteristics, as shown below.

### Publication Trend

To begin, we sought to see if the publication years of the final studies aligned with the upward trend depicted by the Google Scholar search in Appendix A. Figure 3 shows that although the first article in this report was published in 2006, there was not a spike in publications on cyber insurance until after 2016.

**Figure 3**  
PUBLICATION YEARS

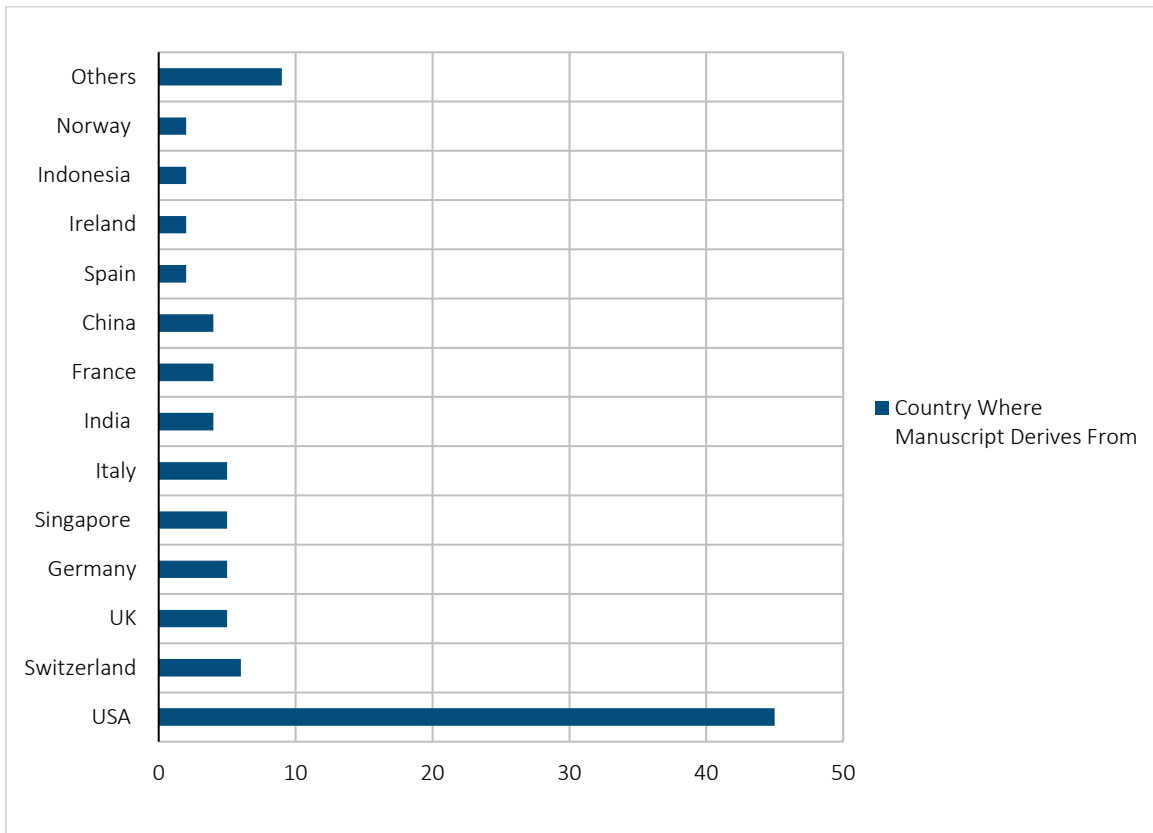


### Manuscript Location

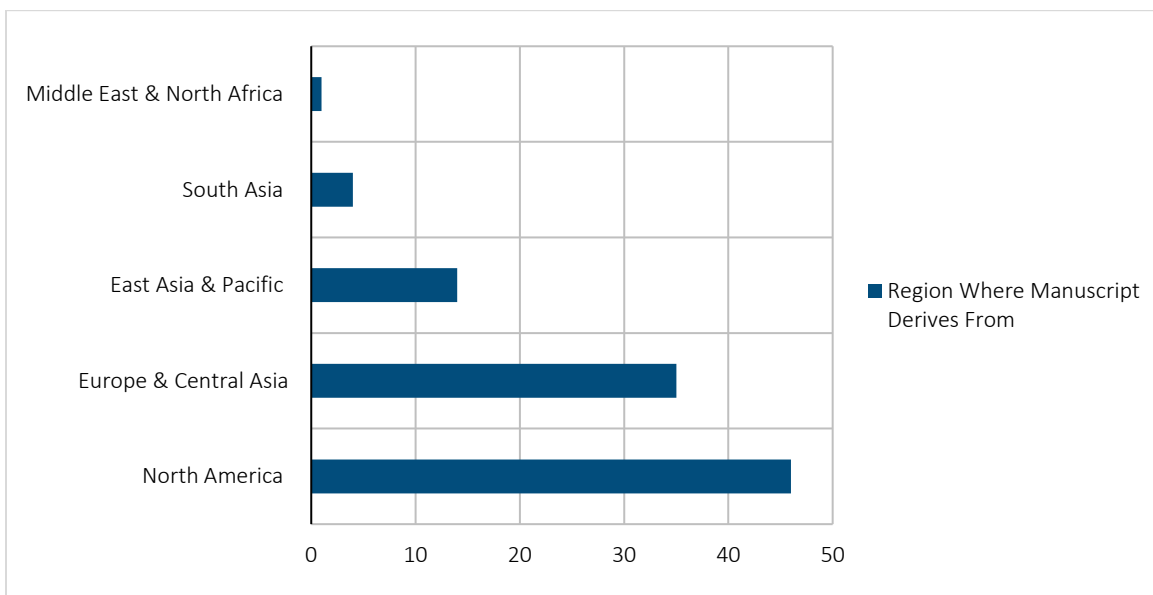
Next, we investigated the countries and regions the manuscripts derived from based on the affiliation of the first author (Figures 4 and 5). In the body of literature in this report, an overwhelming majority of the studies are derived from the United States (U.S.) and North America. Although other countries and regions were accounted for, even then, many of the studies focus on U.S.-based datasets or analyses of U.S. data.



**Figure 4**  
COUNTRY MANUSCRIPT DERIVES FROM



**Figure 5**  
REGION MANUSCRIPT DERIVES FROM

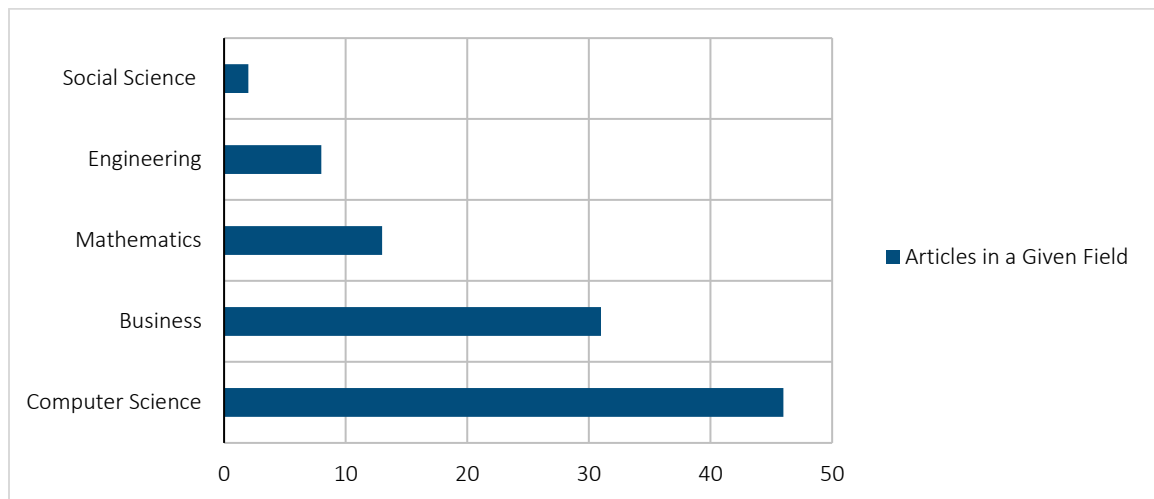


Regions stem from World Bank categorization

## Field Categorization

From there, we generalized the Web of Science categorizations to depict the field in which each study was best suited (see Figure 6). For those studies that were not found on the Web of Science, we used their methodologies and results to best align them with studies that were already categorized on the Web of Science. The generalization of the searches resulted in field categorizations of Computer Science, Business, Mathematics (i.e., actuarial science studies were based in Mathematics), Engineering, and Social Science. As depicted in previous literature, most of the research in this space is based in computer science with limited studies in actuarial and social sciences.

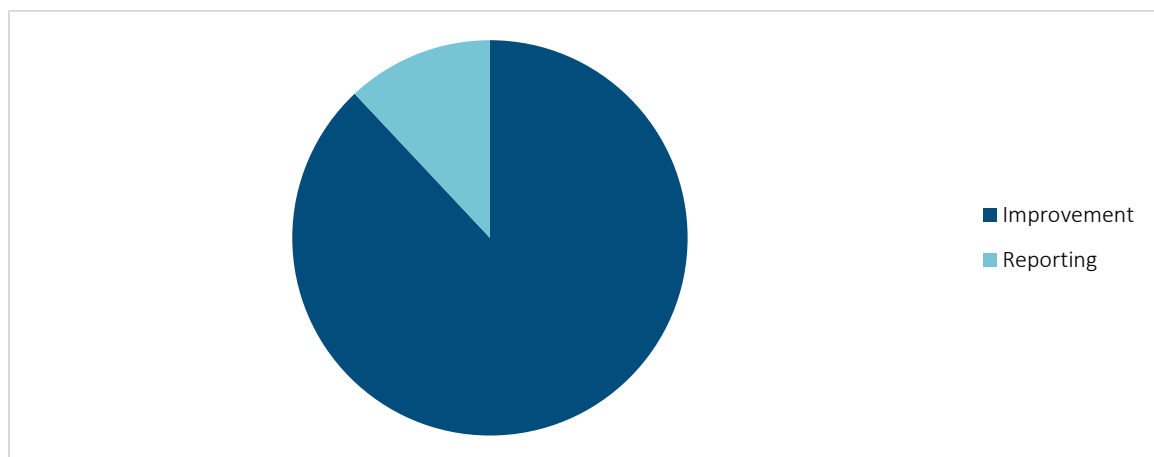
**Figure 6**  
FIELD CATEGORIZATION



## Study Aim

A majority of the studies in this review aimed to improve a method towards quantifying cyber risk or arriving at new cyber insurance methods. As Figure 7 highlights, improvement was the main aim of a large percentage of the studies, while 12 of the articles reported on existing methods used to address cyber insurance.

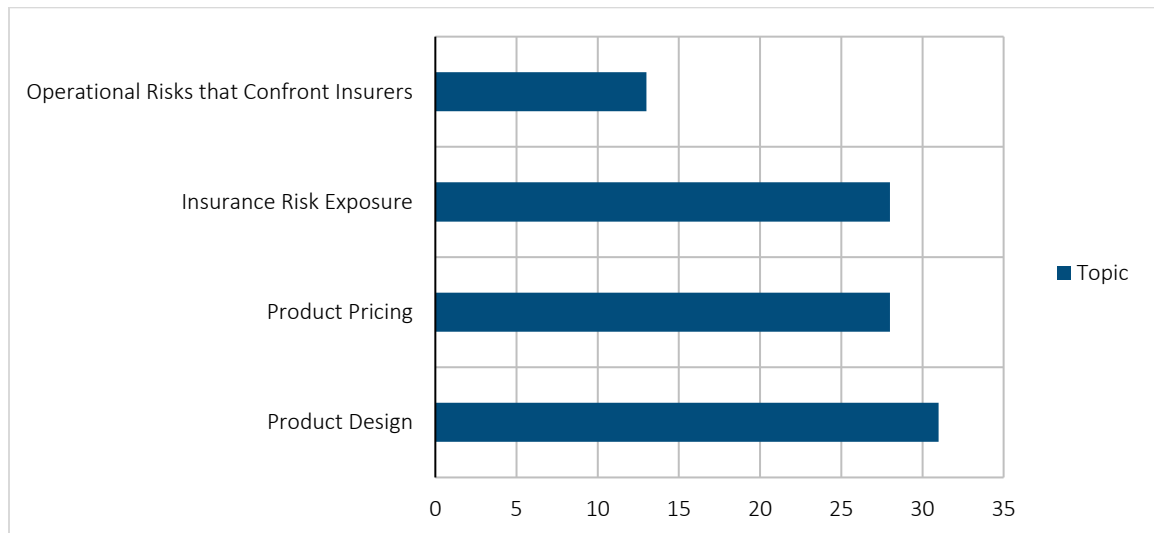
**Figure 7**  
STUDY AIM



## Topic

Based on the objectives of this study, we sought to differentiate between the two distinct perspectives that have been key to the insurance industry for years – product design/ pricing and managing risk exposure and addressing the operational risks that confront insurers. According to Figure 8, the first perspective taken from the design/ pricing and risk exposure angle encompasses a majority of the studies. Likewise, operational risks that confront insurers are only present in eight studies.

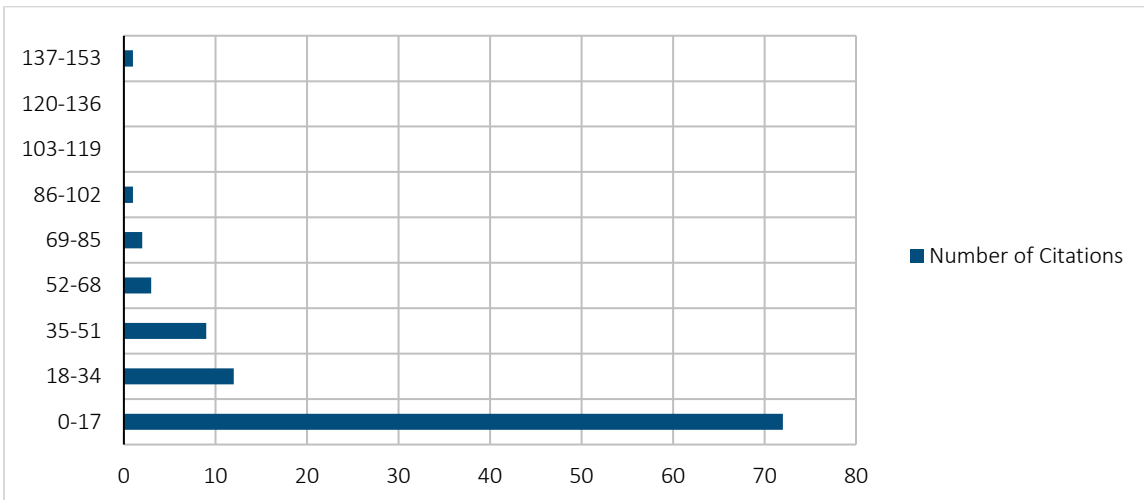
**Figure 8**  
TOPIC



## Number of Citations

In the analysis, we also recorded the number of citations each article received. In Figure 9, we sought to show the histogram of the number of citations per article. It is important to note here that over half of the articles were published during 2021 or 2022, which could account for the lower or nonexistent citation rates.

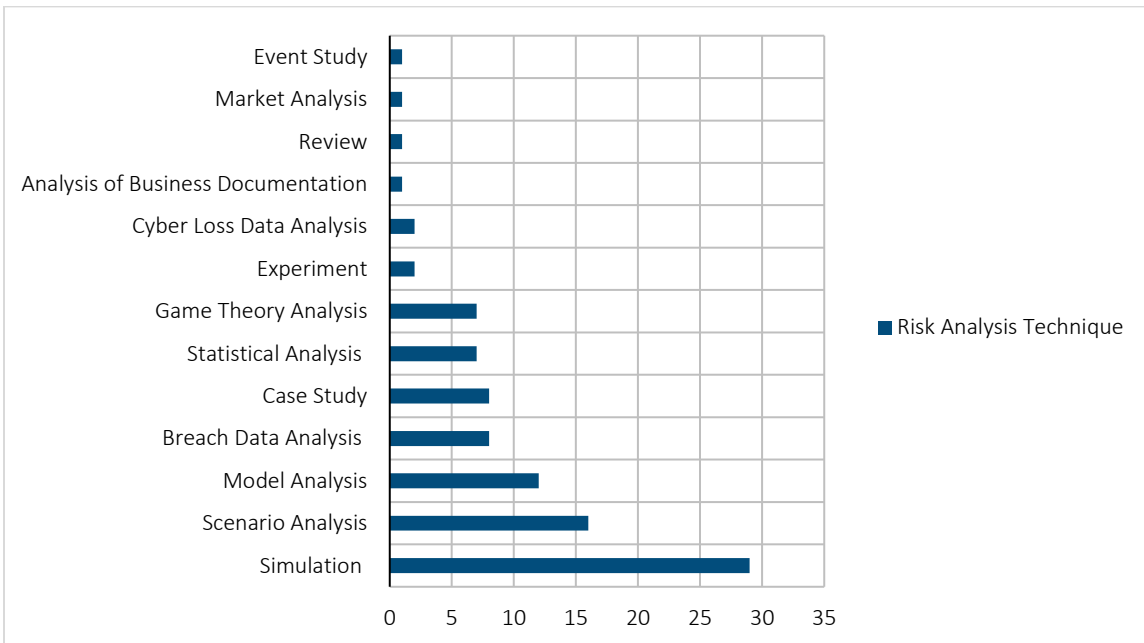
**Figure 9**  
NUMBER OF CITATIONS



**Risk Analysis Techniques**

Prior to understanding the models and methods used in the cyber insurance literature, we analyzed the risk analysis techniques utilized in the studies. Here, Figure 10 shows the breakdown of the risk analysis techniques based on their frequency, where simulations, scenario analysis, and model analysis were most frequently used.

**Figure 10**  
RISK ANALYSIS TECHNIQUES



## Section 4: Modeling & Pricing Methods

Through the review of the literature, we identified various methods for modeling and pricing cyber insurance. These include simulations, game theory, network models, case analysis, statistical analysis, and non-intrusive risk scoring. We, first, seek to discuss the three types of cyber risks – Idiosyncratic, Systemic, and Systematic. We, then, explore the various modeling methods used, highlighting their generalizability, limitations, and pros/ cons.

### 4.1 NON-SYSTEMIC RISKS VS. SYSTEMIC VS. OPERATIONAL RISKS

Due to the ever-increasing nature of cyber risks, classic insurance models and frequency-severity assumptions are no longer appropriate. As such, the frequency-severity approaches must be customized for particular businesses or risks. Such categorization of risk can be subdivided into systemic risks, non-systemic risks (i.e., idiosyncratic, systematic), and operational risks.

In cyber insurance, *systemic risks* have been identified as “cyber risks resulting from being a part of a network; for example, malware or supplier attacks” (Awiszus et al., 2021, p. 3). Similarly, Zeller and Scherer (2021, p. 20) define systemic events as “incidents at multiple firms at the same time and, if of malicious origin, are typical of an opportunistic nature.” Such an attack often stems from a shared vulnerability, which extends the modeling beyond the classic actuarial frameworks. Widespread attacks such as NotPetya ransomware, Kaseya zero-day vulnerability, and the Dyn Distributed Denial of Service (DDoS) attack can be considered systemic cyber risks since they affect many organizations that are not necessarily related to each other (European Systemic Risk Board, 2020; Forscey et al., 2022). Lack of insights into exposure to systemic cyber risks might lead to underinsurance that can be overcome via data science and telematics (QOMPLX, 2020).

There are two types of non-systemic cyber risks: idiosyncratic and systematic. *Idiosyncratic cyber risks* are “cyber risks that occur at individual policyholders – independently of the other firms; thus, they are subject to pooling of risk” (Awiszus et al., 2021, p. 3). Examples of such attacks include targeted or tailored attacks toward that particular entity. Modeling of idiosyncratic risks relies on the entity’s inherent characteristics. A cyber incident like Stuxnet can be considered an idiosyncratic risk event since it is only effective on a specific target organization.

The second type of non-systemic risks is systematic risks. *Systematic cyber risks* are “cyber risks resulting from common vulnerabilities of the insured; therefore, they affect different firms at the same time, e.g., due to utilization of the same software, server, or computer system” (Awiszus et al., 2021, p. 3). Such risks can be modeled using common risk factors. For example, if an application server is used by three different organizations for specific purposes, when the server is down due to an attack, it would disrupt all three organizations, but no other organizations would be affected by this systematic incident.

Systematic risks are modeled by network models that capture interconnectedness and cascading propagation and game-theoretic models. Cyber network models consist of a network, spread process (i.e., epidemic spread process, Markovian spread models, non-Markovian spread models), and loss model.

Table 1 provides examples for each type of cyber incident.

**Table 1**  
CYBER RISK CLASSIFICATION EXAMPLES

	Idiosyncratic Cyber Incidents		Systematic Cyber Incidents		Systemic Cyber Incidents	
	Targeted attack	Individual failure	Targeted attack	System Failure	Untargeted attack	Mass failure
<b>Data Breach</b>	Targeted data theft	Individual unintended data disclosure	Targeted data theft towards a specified system	Unintended system data disclosure at a small cloud service provider	Data theft through widespread malware/phishing	Unintended data disclosure at a large cloud service provider
<b>Business Interruption</b>	Targeted Ransomware attack	Disruption of IT system or process through accidental malfunction	Attack disrupting systems depend on the same software	Systems' disruption due to the software failure	Widespread ransomware attack	Cloud service outage disrupting business services
<b>Fraud</b>	CEO fraud through targeted whaling attack	Accidental compromise of a database by an employee	Database compromise by an employee of a small cloud service provider	Failure results in database compromise at a small cloud service provider	Widespread ransomware attack or social engineering fraud	Accidental compromise of data stored at a major cloud service provider

Adapted from Zeller and Scherer, 2021

Operational risk is defined as the risk of loss due to failed internal processes, people, systems, or external incidents (Egan et al., 2019; Jarrow, 2008). They usually increase with complexity due to the increased number of “vulnerabilities, security threats, and potential associated impacts” (Carfora et al., 2019, p. 5). Cebula and Young (2010, p. 1) define cyber risk as “operational risks to information and technology assets that have consequences affecting the confidentiality, availability or integrity of information or information systems.” Thus, cyber risk is a subgroup of operational risk. Cebula and Young (2010) also presented a taxonomy for operational risks that could be useful for cyber risk modeling.

In the following subsection, the studies in the literature are classified based on the methods they utilized to assess the aforementioned types of cyber risks.

## 4.2 METHODS

In the review of the literature, several methods of modeling or pricing cyber insurance were presented. The methods utilized in cyber insurance research include actuarial methods, simulations, game theory, network models, case analysis, statistical analysis, non-intrusive risk scoring, and artificial intelligence (AI) or machine learning techniques. Studies that employ multiple methods are analyzed and cited under each of the relevant cyber risk modeling and pricing method category.

### 4.2.1 TRADITIONAL ACTUARIAL THEORY AND PRACTICE

Romanosky et al. (2019) conducted a thematic analysis of the contents of various cyber insurance policies on the SERFF system filings provided by NAIC and detected five main themes that insurers used for calculating premium prices: (i) depend on external sources, (ii) estimated, (iii) compared with competitors' prices, (iv) used the experience of their underwriters, and (v) adapted prices from other insurance lines. Based on the 69 policies analyzed by Romanosky et al. (2019), the cyber insurance premiums are calculated

via four main approaches: flat rate, flat rate with hazard groups, base rate, and base rate with security questions. More than half of the policies in the sample utilize the base rate with security questions approach (Romanosky et al., 2019). Results also suggest that the firm's asset value is the most important characteristic in computing insurance premiums, which presents the largest proxy for risk.

Böhme et al. (2019) conduct an interdisciplinary review of the literature on cyber risk analysis to differentiate cyber risks from conventional risks. From the review of the literature, the study defines cyber risk and discusses treatment options, current economic modeling, and actuarial modeling of cyber risks. The study presents new methods for modeling cyber risk with an emphasis on the driving factors.

Carfora et al. (2019) seek to investigate the peculiarities of cyber insurance pricing from the insurer and insured perspectives. Via scenario analysis, the study takes an economic perspective which offers an estimation of the premium based on actuarial principles and indifference premium, which is the max the insured is willing to pay.

Saini et al. (2011) use the utility theory model to conduct a premium calculation of the cyber risks presented to two distinct universities – one in the U.S. and the other in India. It has been determined that the utility method can be an effective tool for insurance companies to design insurance products based on the risk profiles of universities.

Sharma & Mukhopadhyay (2022b) presents a time-series-based Cyber Risk Assessment and Mitigation for Smart Cities (SCRAM) model based on the Protection Motivation Theory comprising three modules. The model proposes strategies to reduce cyber risk using technology (i.e., the use of perimeter security to deter cyber threat actors from disrupting smart traffic flow) and pass the residual cyber risks to third-party cyber-insurers.

Sheehan et al. (2021) propose a conceptual cyber risk classification and assessment framework using a bow-tie model and risk matrix to demonstrate the significance of barriers to reducing exposure to cyber risk. Using both historical data and expert opinion, this model highlights both cyber weaknesses and actions that should be taken to bolster cyber defenses.

Verlaine (2021) developed an extreme risk modeling method to extract information about cyber risk distributions from structured financial products. It is shown that if structured products exist, observed market prices correctly reflect expected losses, given the market is efficient.

Yang et al. (2019a) proposes a model based on principal-agent theory aimed at monitoring signals for cybersecurity information sharing. It is shown that by "introducing monitoring signals, the insurer can collect more information about the effort level of the insured and encourage the insured to share cybersecurity information based on the information sharing output and monitoring signals of the effort level" (2019).

#### 4.2.2 SIMULATIONS

Simulation is defined as "the process of designing a model of a real system and conducting experiments with this model for the purpose either of understanding the behavior of the system or of evaluating various strategies (within limits imposed by a criterion or set of criteria) for the operation of the system" (Shannon, 1975). Various simulation methods have been used by actuaries for analyzing models with high complexity or when there is a lack of data. The system is imitated by breaking down to its components, and the effects of the changes in the values of various parameters are observed instead of utilizing analytical solutions or conventional numerical approaches (Daykin et al., 1993). One of the most used stochastic simulation approaches in the insurance industry is Monte Carlo simulation, where random number generation is

utilized for various parameters based on known or assumed distributions. Uniform distribution is usually used for the random number generation for one or multiple factors. An approximation to a numerical estimate for the overall system can be made based on the simulation model. Monte Carlo simulations are widely used in cyber insurance modeling as well. For portfolio selection, simulation approaches are deemed valuable to augment asset allocation decisions to assist mathematical models (Booth et al., 2020).

Monte Carlo analysis is beneficial for implementation with the correlation risk analysis (Wang, 1997). Another advantage of the Monte Carlo simulation is its fit for analyzing epidemics spreading over the nodes of a network (Xu & Hua, 2019). Simulation models are also used for generating loss distribution under cyber-attacks to analyze the losses under various conditions for cyber insurance purposes (Johnson et al., 2014).

A disadvantage of the simulation approach is that it is only good when the simulation model, correctness of the input data, and relevant distributions well represent the real-world system (Carfora & Orlando, 2019). Deficiencies regarding either of these components of a simulation model would result in misleading estimates. Moreover, building, running, and analyzing Monte Carlo simulations can be very time-consuming.

Bohme and Kataria (2006) discuss the factors influencing the correlation between cyber risks at both the global and individual levels. Using t-copula and simulations to model cross-firm risks, it is found that while global risk correlation influences insurers' decision to set the premium, the internal correlation within a firm influences its decision to seek insurance. They conclude that cyber-insurance is thus best suited for classes of risk that have a high internal and low global correlation.

Erdogan et al. (2017) presents a method for developing executable algorithms for quantitative cyber-risk assessment. The study presents CORAS, a model-driven risk analysis that is calculated using Monte Carlo simulations. The model is validated using scenarios where it is the model and algorithms were found to be easy to understand and beneficial to assessing cyber risk costs.

Fahrenwaldt et al. (2018) presents a novel approach to pricing cyber insurance contracts by presenting the first mathematical model of insured losses caused by infectious cyber threats. The model is based on the exact loss model and polynomial and mean-field approximation and validated via Monte Carlo simulations. The model emphasizes the impact of the network topology, indicating the notion that higher-order approximations are crucial for the analysis of non-linear claims.

Liu et al. (2021) presents an actuarial framework using the semi-Markov process to capture and reduce the riskiness raised by interdependence among cyber risks to enhance the cyber insurance market for power systems. Using Monte Carlo simulations, both the individual premiums and the impact of self-protection are found to be significant.

Lu et al. (2018) presents a cyber insurance framework using Poisson statistical analyses to transfer cyber risk to a third party. Through the framework creation and Monte Carlo simulations, it is found that transferring cyber risk presents challenges due to premium and indemnity calculations, cyber risk correlation, insurability, and compensation of secondary loss.

Pal et al. (2021) presents a foundational methodology for determining the effect of individual heavy-tailed and tail-dependent cyber risks on the cyber market. Monte Carlo Simulations are run on the Chronology of Data Breaches dataset provided by the Privacy Rights Clearinghouse (PRC). It has been found that spreading heavy-tailed cyber risks that are not catastrophic is an effective practice for cyber risk management.



Pate-Cornell & Kuypers (2021) present a probabilistic risk analysis model based on the existing SpaceCorp incidents and new attack Monte Carlo simulations. A full risk curve is found that allows for the allocation of cybersecurity resources meant for different attacks.

Shah et al. (2015) presents the minimum value of data security or privacy for a customer using a classical loss distribution approach. Via Monte Carlo simulations, it is found that the minimum bound on the value of the security is not only determined by the cyber insurance premium charged but the customers' own risk aversion.

Xu & Hua (2019) develop a framework for modeling and pricing cybersecurity risk using epidemic modeling techniques. With the proposed model, simulations are run to evaluate the security level of networks, and the security level includes the number of incidents, the infection probabilities of nodes, and the total losses.

Xu & Zhang (2021) investigate data breach catastrophe (CAT) bonds via a multiperiod pricing model. Through simulations, it shows data breach CAT bond can be an attractive financial product and an effective instrument for transferring the extreme data breach risk.

Yang et al. (2020) presents a framework of premium calculation for cyber insurance businesses by modeling potential electronic intrusion. The study establishes cyber insurance premiums through simulations to highlight the correlation of problematic combinations of disruptive switching cyberattacks.

Zeller & Scherer (2021) developed an actuarial model based on a holistic loss distribution approach to cyber risk. The resulting model simulations capture accumulation risk stemming from multiple firms simultaneously affected by a cyber event.

Zhang et al. (2021) propose cyber insurance for the cyber risk management of water distribution systems using a semi-Markov process model. Via sequential Monte Carlo simulations and case studies, higher system reliability and more advanced self-protection mechanism are shown to reduce the cyber-insurance premium of the water utilities in question.

#### 4.2.3 GAME THEORY

Game theory provides a powerful decision-making framework that can be used for analyzing the outcomes of the decisions of different actors (Marotta et al., 2017). Since risk exposure of entities is usually interdependent due to the influence of other parties' decisions, game theory is widely used in the insurance field for various purposes (Awiszus et al., 2021).

Game theoretical models have been developed in cyber insurance modeling. There are various ways to implement the game theory for cyber insurance that could be useful for insurers, agents with or without insurance, and regulators. Game theoretical models can also be applied to situations where asymmetrical information exists among entities.

The aspects of game theoretical models that still need to be improved include modeling of catastrophic cyber risks, analysis of heterogeneous cyber networks, and analysis of the heterogeneous impact of cyber incidents. The disadvantage of the current game theoretical models is the oversimplification of the real-world systems to be applied to game theory (Awiszus et al., 2021).

Acharya et al. (2021) propose cyber insurance for Electronic Vehicle Charging Stations (EVCSs) to mitigate losses from cyber risks and design a model for public stations. Using game-theoretic modeling and optimization, risk assessment techniques, and case studies risk assessments are found to be crucial for

designing insurance premiums, where insurance premiums increase in alignment with the loss coverage offered by EVCSs. Yet, due to limited publicly available data on EVCS cyberattacks, Acharya et al. model the Weibull distribution parameters using data from cyberattacks in the information technology industry, consistent with the current real-world practice where limited data presents a challenge.

Feng et al. (2021) model a fog computing platform for APT attacks as a Stackelberg game framework. It is found that dynamic strategies, as presented by the fog computing platform, have a higher payoff for the fog computing provider, higher profit for the cyber insurer, and less payoff for the attacker.

Similarly, Feng et al. (2021) propose a novel approach to cyber risk management for blockchain-based services using a two-level Stackelberg game-theoretic approach. It is found that the blockchain provider and the cyber-insurer need to set their pricing/investment strategies, and then the users follow to determine their demand for the blockchain service.

Shetty et al. (2010) investigates how competitive cyber insurers affect the security and welfare of a networked society via the utility theory model. It is found that although cyber insurance improves user welfare, competitive cyber insurers fail to improve network security.

Feng et al. (2018) study a competitive pricing problem via a Stackelberg game approach for which firms compete for selling substitutable cyber-insurances. The study finds that "the cyber-insurer, who provides the security service with higher quality than other cyber-insurers, earns more profit in the market with strong interdependency than that in the market with weak interdependency while other cyber-insurers earn less profit simultaneously" (2018).

Hayel & Zhu (2015) presents a new cyber insurance model that considers the complex interactions between users, attackers, and the insurer. Using a games-in-games framework, the study captures the interactions and presents guidelines for designing insurance policies. The study finds that the propagation of the asymmetry through either action or inaction of a user can provide security benefits that can be measured via utility.

Johnson et al. (2014) seeks to address the problem of systematic risk by analyzing the systematic risk of a networked system that is subject to both direct risks based on individual investments and indirect risks based on the network's topology. The study borrows a risk propagation model from the literature on interdependent security games using simulation algorithms to approximate loss distribution. The study finds that the loss distribution derived from this study differs significantly from a standard binomial distribution. In this, the risk of a catastrophic event was higher if the nodes compromised were independent events.

Khalili et al. (2018) investigate the possibility of using cyber insurance as an incentive for improving network security via a game-theoretic approach. It is found that security interdependence among agents seeking cyber insurance leads to a profit opportunity for the insurer.

Khalili et al. (2017) seek to answer how, when faced with risk dependency whether an insurer should underwrite both the client and vendor or only one party, leaving someone else to underwrite the other dependency. Using a simple two-agent, two-insurer model, it is found that there is a benefit to insuring both.

Khalili et al. (2019) investigate how cyber risk dependencies can be taken into consideration when underwriting cyber-insurance policies using a standard underwriting framework. Using a scenario-based approach, it is found that the insurer's best strategy for managing cyber risk dependencies is to underwrite both the network service provider and its customers.

Khalili et al. (2019) designed a game-theoretic cyber insurance framework under the contract theory framework based on the attack model to investigate breach or loss challenges. From scenario analysis, the study finds that post-screening is not effective with rare losses while prescreening is effective if the agent perceives the loss as rarer than the insurer. Here, pre-screening improves both the agent's effort and the insurer's profit.

Laszka et al. (2018) presents a math-based assessment of systematic risk in networked systems based on a game-theoretic approach. Using a multiple-hop propagation model, the study simulations found the full network possesses systematic risks, which may require large amounts of safety capital to properly insure.

Laszka et al. (2014) sought to find general rules for calculating the risk exposure of nodes within a connected system using network risk models which build on game-theoretic approaches. In analyzing two independent real-world systems, structural regularities are found to help improve the prediction of cyber risks.

Lau et al. (2021) introduce coalitional insurance as an alternative to traditional insurance plans using game-theoretic algorithms and attack graphs. Under the proposed cyber-insurance model, several aspects of an insurance policy, where said premiums are determined through analysis of system vulnerability and losses. As presented in the case studies, higher defense levels of entities are incentivized by reduced insurance premiums.

Liu (2021) presents a review of the cyber insurance field via a variety of insurance contract models and game-theoretic approaches. The book highlights the validity of using insurance as an effective tool to control cyber risk.

Pal & Golubchik (2010) address the problem of optimal cyber insurance contracts between the insurer and the insured to maximize both welfare and profit. Via game-theoretical modeling, it is found that the optimal premium for monopolistic insurers is more than social welfare-maximizing insurers, where welfare-maximizing insurers charge a fair premium to those that are sure to face a risk.

Pal & Hui (2012) proposes a game-theoretic mechanism to address the challenge of appropriate premium modulation based on the user risk type. It was found that the optimal fine/ rebates per user should be allocated in proportion to the centrality of the user.

Pal et al. (2019) propose a Stackelberg game pricing environment consisting of security vendors and their clients to determine levels of investment and accountability. It is found that a monopoly security vendor could improve their current profit margins by 25% if they accounted for their client's location and investment info.

Schwartz & Sastry (2014) presents a game-theoretic framework for managing cyber-risks in large-scale interdependent networks. The study finds that cyber insurance alone is not a beneficial means of improving security; instead, incentives and other aspects must be implemented to improve security.

Wang et al. (2021) provide a theoretical framework for cyber insurance using game theory to calculate the monetary value of risk and insurance premiums associated with software compromise. The paper finds insights into estimating cyber insurance and shows its efficacy on real malicious app data.

Zhang & Zhu (2020) proposes a bi-level game-theoretic framework, called FlipIn, to design incentive-compatible and welfare-maximizing cyber insurance contracts. Through model and scenario analysis, the importance of network connectivity in the security of IoT devices and the insurability of defenders is shown.

Zhang et al. (2017) presents a bi-level game-theoretic model to capture complex interactions between a user, an attacker, and the insurer. This study finds a fundamental limit on insurability, predicts the Peltzman effect, and shares the principles of zero operating profit and linear insurance policy of the insurer.

#### 4.2.4 NETWORK MODELS

Network theory is the study of graphs where entities and their relationships are taken into consideration. Network models are employed by the insurance industry to analyze the cascading propagation and effects of interconnections among entities. Network models in the insurance field can comprise of nodes that are organizations (insurer, agent, regulator) or, with more granularity, single devices and edges that represent the relationships among the nodes (Aviszus et al., 2021; Eling, 2020).

Network models provide the ability to analyze the spread of cyber incidents that are useful for the cyber insurance industry to study systemic cyber risks. With the addition of a loss model for each node, the network model can analyze the severity of disruption over the network. However, the loss models have usually been kept simple by studies in the literature and are open to improvement with future research (Aviszus et al., 2021).

Antonio et al. (2021) use a graph-mining technique for cyber insurance ratemaking on weighted networks to obtain more competitive cyber insurance pricing. Using the susceptibility-infectious-susceptible model, more reasonable and competitive heterogeneous premiums are found. The prices found with graph mining are lower than those without GMA graph mining approach and communication factors.

Antonio et al. (2021a) presents a novel Markov-based model using epidemic spread functions to determine the influence of clustering on calculating cyber insurance premiums. Through simulations, it is found that this calculation method is more comprehensive since it considers two network properties, including the degree and local clustering coefficient.

Tatar et al. (2020) developed a graph-based cyber risk assessment model that integrates attack propagation and impact propagation analysis. Using Bayesian attack graph methodology along with the Common Vulnerability Scoring System, possible attack paths and the likelihood of a successful breach can be computed using this model. The likelihood of incidents is also integrated with impact propagation from the assets of an organization to the business processes can be calculated using the Functional Dependency Network Analysis methodology, enabling the cyber insurers to compute the cyber risk of an organization.

Awiszus et al. (2021) presents a survey of modeling and pricing of cyber insurance for varying cyber risks using a frequency-severity approach drawing on dependence modeling, spread models, and game theory. The study distinguishes between three types of cyber risks – idiosyncratic, systematic, and systemic. It is found for non-systemic cyber risks (i.e., idiosyncratic and systematic), classic actuarial modeling is sufficient, yet systemic cyber risks require a more complex modeling technique based on epidemic spread models. As cyber risks increase and threat vectors expand, Awiszus emphasizes cyber insurance pricing techniques that include interdependence for both systematic and systemic cyber risks using risk-neutral valuation and risk measures (i.e., epidemic model solutions and top-down approaches).

Hillairet & Lopez (2021) propose a framework aimed at managing insurance risk exposure towards systemic risks of the insurers. The study uses a compartmental epidemiological model to obtain Gaussian approximations for losses. By designing an accumulation simulation mimicking the WannaCry ransomware attack, the study models the impact of a large cyber-attack on insurance portfolios. The model presented serves as a tool to quantify the gain obtained through various reaction and preventative strategies.

Insua et al. (2018) review three major decision problems relevant to cybersecurity economics via model analysis. The study examines the three models using influence diagrams and bi-agent influence diagrams to create a framework for estimating the economic impact of cyber risks that buyers of insurance and insurance companies face.

Li et al. (2020) explores the discouragement attack model within the point-of-sale mechanism in blockchain networks and adopts cyber-insurance as an incentive for motivating the validators' online duration using the contract theoretic framework. The design of the system proves the feasibility of the contracts and presents the optimal results in the simulation. It has been found that validators can obtain insurance claims without paying the premium, and blockchain networks can keep validators online to defend against attacks under the proposed insurance contract.

Hua & Xu (2021) propose an innovative approach to pricing cyber insurance for a large-scale network. The study uses static scale-free random graphs and linear and generalized models to study the sequential occurrence of infection and recovery as well as the time until infection. Using synthetic data, they develop a simulation-based approach for which simulations are run, and a case study is presented to show the algorithms used in cyber insurance pricing.

Jevtić & Lanchier (2020) propose a graph-theory structural model of aggregate loss distribution for cyber risk of small to medium-sized enterprises. Using tree-based LAN topology, the study presents the first theoretical model of aggregate loss distribution for cyber risk in small to medium-sized environments. The results of this study present an exact expression of the expectation of aggregate losses due to a cyber data breach, holding for all parameters of a system.

Lau et al. (2022) presents a novel cyber insurance model design based on system risk evaluation with smart technology applications. The model is based on a stochastic epidemic network model and cooperative game approaches and is tested using a simulation. It is found that "smart monitoring and job thread assignment solutions can work standalone or together to boost the reliability" of transmission grids (2022).

Shetty et al. (2018) presents a cyber risk scoring method using Bayesian attack graph models to assess the security of the insured to provide insight to the insurer for pricing. The Cyber Risk Scoring and Mitigation (CRISM) tool presented produces risk scores that allow firms to choose the optimal mitigation policies to reduce insurance premiums.

Cutler et al. (2017) provide a model to calculate the likelihood of cyber incidents for cyber insurance pricing purposes. This model applies Markov chain analysis on Lockheed Martin's cyber kill chain to calculate the probability of failure of the cybersecurity product. This model is an example of the adoption of reliability engineering approaches for use in cyber risk assessment.

Kaffenberger and Kopp (2019) present a conceptual framework to assess country-level systemic cyber risks. The framework provides an illustrative index of cybersecurity, cyber risk exposure, and resilience.

Hoffman (2018) provided the models to measure accumulation risk that is more focused on large incidents. Exposure measurement and claims cost assessment are integral parts of managing accumulation risks. The high interconnectivity of cyber risks plays an important role in modeling accumulation risks.

Zhang et al. (2021) developed a model to analyze the cyber risks of fog networks by considering the risk propagation mechanism. They used an interval approximation method for quantification of frequencies of network elements in an IoT smart home network. This method can be used for pricing insurance risk using the frequency-severity approach and actuarial pricing principles, including expectation, standard deviation, and Gini means difference principles.

#### 4.2.5 CASE STUDY

A case study is defined as an “in-depth study undertaken of one particular ‘case,’ which could be a site, individual, or policy” (Green & Thorogood, 2018). A case study aims to explore an event or phenomenon in its natural context (Crowe et al., 2011). The case study approach is used by the insurance industry for real cases or hypothetical cases that are realistic to analyze what could happen.

Case studies are useful for studying the risks of extreme events when undertaking a formal experimental investigation is not possible (Crowe et al., 2011). Potentially huge losses related to systemic cyber risks are examined by case study analysis (Eling, 2020). Comparisons can be conducted using such case studies in the literature.

The case studies in the academic literature include:

Carfora & Orlando (2019) propose the first approach aimed at estimating both Value at Risk and Tail Value at Risk. The study conducts a case study using the “Chronology of Data Breaches” dataset provided by Privacy Rights Clearinghouse (PRC), modeling loss frequency via Poisson and negative binomial distributions and modeling the severity of data breaches using lognormal and skew-normal models. To test the frequency distributions found via statistical analyses, both historical and Monte Carlo simulations are run, confirming the good fit for the severity distribution. They find that estimating cyber risks via Value at Risk or Tail Value at Risk results in higher empirical estimates and a more conservative prediction of the losses.

Similarly, Carfora & Orlando (2022) further the 2019 study by providing insights on the statistical distributions of the severity and frequency of data breaches. The study conducts a case study using the “Chronology of Data Breaches” dataset provided by Privacy Rights Clearinghouse (PRC), modeling loss frequency via Poisson and negative binomial distributions and modeling the severity of data breaches using lognormal and skew-normal models for both malicious and negligent data breaches. It is found that data breaches of diverse types often show different statistical natures, especially if occurring at different entities.

Carfora et al. (2019) investigate the peculiarities of cyber insurance pricing from both the insured and insurer perspective. They use the “Chronology of Data Breaches” dataset provided by Privacy Rights Clearinghouse (PRC) as an illustrated example, modeling breach frequency with Poisson and negative binomial distributions models and breach severity with lognormal and skew-normal models. In modeling the frequency-severity of data breaches, the study presents an estimation of cyber insurance premiums based on actuarial principles and indifference premiums, which is the maximum the insured is willing to pay.

Egan et al. (2019) propose a framework to assist insurance organizations in cyber operational risk management using scenario development. Using the framework, three detailed scenarios are modeled, providing a consistent scenario development method and common taxonomy.

Insua et al. (2021) presents a framework for adversarial risk analysis utilizing both intentional and nonintentional threats. Via a defense-attack case study, the study presents a comprehensive risk analysis based on a multiagent influence diagram.

Piromsopa et al. (2017) propose a scoring model for cyber insurance based on the results of internal and external audits and compliance with standards. The study utilizes a case study, which further shows that certain cyber threats can be mitigated and that although the risk may exist, insurers should lower the premiums for customers with standard compliance.

The case study approach helps government agencies facilitate workshops for critical infrastructure operators to analyze the effectiveness of cyber insurance (CISA, 2014a).

Watson et al. (2022) take a mixed-method approach to understand the purchase of cyber risk insurance and enhancement of operational cyber risk mitigation programs by interviewing New Jersey bank officials. It is found that most of the cyber insurance variables in this study had either a random or negative impact on operational cyber risk mitigation programs.

Welburn & Strong (2021) presents a theoretical input-output framework and model to describe systemic risks and cascading failures to estimate the potential economic damage from a cyber incident. Via a case study, it is found that the potential direct costs associated with cyber incidents are greatly outweighed by the multiplier effects.

The use of case studies in the grey literature can be found in the following:

Cambridge Centre for Risk Studies (2019) developed a framework for assessing business interruption risks where various risk scenarios, including cyber-attacks, can be compared. The report conducts a case study analysis on contagious malware infestation and provides insights on how scenario analysis can be useful for cyber risk assessment.

European Systemic Risk Board (2020) provided historical and hypothetical scenarios for systemic risk assessment and came up with mitigation strategies against systemic risks, including developing the capacity to analyze systemic risks, monitoring, data collection and sharing, conducting stress testing, and maintaining clear communication.

Lloyd's (2021a) conducted a cyber insurance case study where three cyber-attack scenarios on industrial control systems can possibly generate major losses for insureds. Although the scenarios are from the manufacturing, transportation, and energy sectors, they can be adopted by other critical infrastructure sectors. The report provides insights on the impact on insurance and reinsurance companies. Three scenarios include various attack types, such as supply chain malware, internet of things vulnerability exploitation, and infiltration over the IT-OT air gap. The implications of the study on the insurance industry are to catch up with the emerging cyber risks in the operation technologies with a growing market.

Lloyd's (2015) presented a case study for the impact of a systemic risk event on the insurance sector – a cyber-attack that causes a large-scale blackout scenario. The scope of the hypothetical scenario covers 93 million people living in 15 U.S. states in the northeast region, including the nation's capital. The total impact on the economy is estimated as \$243 billion to \$1 trillion, based on the severity of the impact. This study provides insights on the implications of direct and indirect impact on insurance losses, with an estimated claims amount of \$21-71 billion. One aspect of the report that is worth consideration is the wide array of claims that might be triggered by such a cyber incident.

Lloyd's (2017b) presents a case study where two different cyber-attacks were analyzed for the interruption of the business. The risk managers of organizations can consider the impact on their own operations by adjusting a range of variables included in the scenarios. For the cyber insurance providers, the report can provide an understanding of the liability and a means for risk aggregation.

In an earlier report by Lloyd's (2010), cyber risks are summarized and succinctly explained. Although the study is from the last decade, its findings regarding cyber risks still apply.

Lloyd's (2018a) focuses on the cyber risks related to the Internet of Things (IoT). Ten scenarios were analyzed to highlight the impact of IoT on the insurance industry, including underwriting, claims, capital

reserving, modeling, and exposure management. The benefits and concerns related to IoT were mapped to the relevant aspects of the insurance industry.

Lloyd's (2021b) provides an intelligence-based study on cyber risks in the aviation sector. The cyber risk exposure identification, quantification, and management in the aviation industry are presented with multiple scenarios.

Lloyd's (2018b) provides insights on the impact on the insurance sector of emerging areas relevant to the cyber domain, such as virtual/augmented reality (VR/AR). VR/AR is a growing market, and the insurance market for such products and services is also increasing. New technologies introduce new risks to human physical and mental health and also to data with new concepts such as metaverse. This technology also has the potential to be used for underwriting purposes, enabling underwriters to examine fields remotely.

Lloyd's (2019a) provides a cyber incident scenario analysis regarding a hypothetical contiguous malware that spreads throughout the world's IT systems and causes a systemic cyber incident. This study presents how the companies, sectors, and society could be exposed and what disruptions can generate losses that relate to the insurance industry. It also highlights the differences between various cyber insurance offerings.

Lloyd's (2019c) presents a scenario analysis where a cyber-attack ceases the operation of multiple Asia-Pacific ports. The impact on the insurance sector is analyzed by estimating the losses in various industries. The report also provides insights on the troubling topics of the silent cyber coverage and underinsurance of cyber risks.

Lloyd's (2017a) developed a systematic approach to model casualty risk accumulation. This stochastic approach models liability exposure, maps the loss scenarios, and provides the economic loss trends for specific loss scenarios. It is useful for all classes of business in any given portfolio. The model represents the relationships in shapes, a kind of graph; then, the relationships are analyzed stochastically.

Lloyd's (2020c) provides a case study for the resiliency of cities and its implications for the insurance sector. Cybersecurity is having more and more importance in resiliency, and insurance is a crucial aspect that is considered for resiliency. The report provides product ideas for the insurance industry, such as umbrella insurance policies, claims data repositories, risk registers, and risk pools.

Ruffle et al. (2014) provide a stress test study analyzing the impact of a catastrophic, low frequency, logic bomb attack on the cyber insurance sector and society. The consequence on the macroeconomic level is a global economic recession. This study is useful for insurers for risk capital assessments. A report by Citi GPS & Cambridge Centre for Risk Studies (2021) gathered such catastrophic stress test scenarios as a resource for insurers.

A report by Risk Management Solutions, Inc. (2016) presents an assessment framework for cyber insurance accumulation risk management. The analysis is conducted in five key cyber loss scenarios, including data exfiltration, denial of service attack, cloud service failure, financial transaction compromise, and extortion. The framework employs the frequency-severity distributions of loss to provide loss estimation for the scenarios.

OECD (2020c) presents a case study regarding the involvement of the government in reinsurance of cyber terrorism incidents. The report highlights the changes needed and the possible challenges regarding the changes for establishing government-backed reinsurance. A similar study by Evan et al. (2017) assesses the threats of cyber terrorism against the insurance sector.



O'Brien et al. (2020) presents a case study with five cyber catastrophe scenarios where the impact on the insurance and reinsurance market is analyzed. This study employed a synthetic portfolio methodology for extrapolation using the existing cyber insurance policies.

Kelly et al. (2016) presents a stress test scenario for cyber risk assessment for critical infrastructure. The scenario is about a catastrophic cyber incident against a regional power supply network, with a broader cascading impact on other critical infrastructure sectors. This method uses the input-output modeling of Leontief for impact propagation.

Kelliher et al. (2017) establish good practices for setting inputs for operational risk modeling for banks, insurance companies, and financial firms. Through a review of regulatory requirements and a literature review, the study recommends analysis of historical loss data and scenario analysis for modeling risks and creating best practices. Further, it is recommended that expert judgment be used for setting correlations and information requirements for mitigation, and allocation of sources be addressed prior to modeling operational risks.

Although not specific to cyber insurance, the findings of two other reports from Lloyd's (2020d; 2020e) are relevant for cyber insurance and provide useful insights regarding the value of reputation and the importance of data on portfolio management.

#### 4.2.6 STATISTICAL ANALYSIS

Statistical analysis is the collection of methods that is focused on collecting, exploring, and presenting large amounts of data to discover underlying patterns and trends" (SAS, 2022). Statistical analysis is essential where data exists. Data is traditionally very important for the insurance industry for risk analysis (Value Momentum, 2022). With the significantly increasing number of data sources, dependence on statistical analysis increases as well (Atluri, 2018). An advantage of statistical analysis is that it has a huge literature along with the developing methods since data is everywhere and all organizations have some data to get insights out of. On the other hand, lack of data is still an issue with cybersecurity data analytics despite the recent efforts to build cyber incident datasets. Another disadvantage of the statistical analysis is that it usually provides insight into the historical data, which does not successfully capture the risks regarding the evolving cyber-attacks (Atluri, 2018).

Bandyopadhyay and Mookerjee (2019) characterize IT risks by proposing an operational model to capture cyber insurance challenges and highlight optimal pricing. By conducting an analysis of myriad breach scenarios and running a numerical experiment, they present a model to capture the impact of secondary loss, finding that the optimal purchase decision depends on a mix of the types of cyber breaches an entity faces.

Barreto et al. (2018) presents a survey of the techniques for managing risks of catastrophic events and the impact of cyber insurance on protecting cyber-physical systems. Using generalized extreme value distribution, it is found that insurance can decrease investments in protection, but under the right coverage (i.e., full liability protection), entities are more motivated to make security investments towards securing cyber-physical systems.

Eling et al. (2022) developed a model to assess the catastrophic cyber risks enabling practitioners to compare various cyber incident scenarios. The model provides a standardized evaluation framework by employing the inoperability input-output model and analyzing the impact of cyber incidents on other sectors based on the interdependencies among sectors. The study found that qualitative context plays a large role in economic impact analysis. Yet, this study is limited in that it depends on various assumptions from subjective expert opinion and uses studies based on historical considerations.

Bessy-Roland et al. (2021) proposes a Multi-variate Hawkes framework to model and aid in the prediction of cyber-attack frequency. Using the “Chronology of Data Breaches” dataset provided by Privacy Rights Clearinghouse (PRC), they modeled the ability to capture self-excitation and interactions of data breaches according to type and target, where a kernel with non-instantaneous excitation provided a better fit. With parsimonious parametric specifications, the model shows reasonable forecasts for a one-year period. Bessy-Roland et al. note that the study is limited as there is no information on the characteristics of breach type or of the breached entity, as well as no financial data.

Carannante et al. (2022) adopts a regulatory perspective to develop a vine copula to capture dependence. Using loss and numerical probability application, they conclude that the dependence structure is an essential feature of price-setting for insurance companies, where a disregard for dependence in cyber risk management may lead to inconsistent estimates of unintended losses. In this, they note that precisely measuring cyber risk exposure requires capturing the interdependency among various cyber risk threats via vine copulas to account for the high dimensionality.

Eling & Jung (2018) raise the question of the dependence structures among different cyber losses. The study uses non-zero pair copula dependence modeling on the “Chronology of Data Breaches” dataset provided by Privacy Rights Clearinghouse (PRC) to model the cross-sectional dependence of data breach losses. The study shows how different high-dimensional dependence constructions influence cyber insurance premiums and cyber risk assessments, highlighting the importance of determining risk factors in underwriting and cyber risk management.

Eling & Jung (2022) uses the SAS OpRisk dataset of operational risks to model cyber losses using the Tweedie regression-based model to model the best fit for cyber loss severity in the financial industry. It is found that operational risks in the financial industry should reflect the statistical features of firms' individual risks. In this, financial firms that have increased firm size, those that face operational risk effects that affect multiple firms, and higher liability costs are statistically more likely to face greater and more severe cyber losses.

Eling & Loperfido (2017) uses multidimensional scaling and goodness-of-fit tests to investigate the distribution of data breach information. The study utilizes the “Chronology of Data Breaches” dataset provided by Privacy Rights Clearinghouse (PRC) to conduct multi-factor analysis and goodness-of-fit tests. It is found that different types of data breaches need to be modeled as unique risk categories and the skew-normal distribution is a strong indicator of the amount of a data breach. The study is limited in that it focuses on the number of data breaches and the amount of lost data, not the loss of data itself.

Eling & Wirfs (2019) seek to address the question of whether models, which prove beneficial in other loss categories, can be applied to cyber risk and whether cyber risks are structured in any way similar to other risks. Using operational risk databases and cyber incidents extracted from the SAS Global OpRisk dataset and the “Chronology of Data Breaches” dataset provided by Privacy Rights Clearinghouse (PRC), the study uses the peaks-over-threshold method from extreme value theory alongside a loss distribution approach to categorize frequency-loss distributions of extreme cyber risks and those in daily life. It is found that cyber risk constitutes a distinct risk category, where human behavior is the main source of cyber risk, and cyber risks vary greatly from other risks.

Eling et al. (2022) investigates how firm-specific factors interact with the cost of cyber risk events. Using cyber breach data from Cowbell Cyber Inc., quantile regressions are run. It is found that the impact of a firm's revenue is stronger in the lower quantile of the cost distribution, suggesting that mispricing may occur if firms of various sizes use the average effect given by traditional least squared regression.

Erola et al. (2022) presents a system that calculates the Cyber Value-at-Risk of an organization using value-at-risk models and Monte Carlo simulations. The study validates the model via data provided by AXIS insurance company, for which a real case is simulated using harm tree scenarios. The system is found to produce predictions that represent the actual financial loss of an organization.

Farkas et al. (2021) propose a method for cyber claim analysis based on regression trees to identify criteria for claim classification and evaluation. The study used generalized Pareto modeling and extreme value theory and the “Chronology of Data Breaches” provided by the Privacy Rights Clearinghouse (PRC) dataset to identify the distributions and tails. The analysis shows that typical claims should be analyzed separately from extreme ones.

Franke & Draeger (2019) addresses the accumulation risk of business interruption incidents. It presents two simple models, including the incident propagation model and the limited incident management capacity model via Poisson and log-normal distribution.

Gatzert & Schubert (2022) examines the determinants of cyber risk management in the U.S. banking and insurance industry by creating a cyber risk consciousness score via text mining. Using logistical regression, it is found that awareness of cyber risks increased in the subsequent sectors within the time period, where insurers have higher cyber risk consciousness scores.

Jung (2021) proposes a holistic model to determine how big the next data breach cyber loss will be. The study uses generalized extreme value distribution to check the model with the Cowbell Cyber Inc. Data breach dataset. The findings of the data show a significant increase with a break in the loss severity pre- and post-2014. Based on the findings, a three-layer reinsurance scheme based on probable maximum loss estimates is presented.

Lin et al. (2021) provide a framework based on the total loss model to determine how insurance companies should price cybersecurity premiums and how insurance companies can offer contracts that cover the total loss to the firm. Using logistical regression of the Chronology of Data Breaches provided by the Privacy Rights Clearinghouse (PRC) dataset, the study shows how insurers can either use empirical stock return distribution of losses or the per-record cost of a breach to price cyber insurance.

Liu et al. (2022) employ a vine copula approach under the Bayesian framework to co-model incidences from different data breach types. Using two public data sets, including the Chronology of Data Breaches by the Privacy Rights Clearinghouse (PRC) and the Department of Health and Human Services dataset, the study presents simulations that find the overall dependency structure and tail dependence varies between data breaches.

Liu et al. (2021) developed a model based on extreme value theory and applied it to the power grid regarding insurance product design. Via simulations, it is found that the proposed CAT bond design can manage the cyber insolvency risk insurers face when insuring power systems.

Mukhopadhyay et al. (2019) proposes a cyber risk assessment and mitigation framework of risk through cyber insurance. The study computes the loss arising from malicious attacks using collective modeling and generalized linear models.

Palsson et al. (2020) presents a statistical analysis of cyber impacts based on cyber incidents from Advisen cyber loss data. The study shows that exposure to cyber incidents varies between the corporate sector, the relations between entities and cost, and gains insights into cyber risk.

Pooser et al. (2018) examine the statistical trends of cyber risk data from P&C insurers to discuss cyber risk perception. It was found that the early identified cyber risks were the most sensitive to potential disruption based on their size or firm risk.

Bodin et al. (2018) developed a model for risk-sharing that accounts for the common concerns of high deductibles and low ceilings relative to cyber insurance premiums. The study uses risk ladder valuation to determine an optimal set of cybersecurity insurance policies for a firm and aids in selecting the best one. The study is limited in that it did not account for pricing strategies that might be employed by companies selling cybersecurity insurance.

Meland & Seehusen (2018) propose a lightweight, data-driven approach for organizations to determine their need for cyber insurance. A generic risk model is proposed for which a risk profile is used with a cyber insurance profile to estimate the benefit of cyber insurance from various sources.

Poyraz et al. (2020) presents a model to determine the monetary cost of mega data breached on data classified as personally identifiable information (PII) or sensitive personally identifiable information (SPII). This study uses stepwise regression analysis on both the Chronology of Data Breaches dataset provided by the Privacy Rights Clearinghouse (PRC) and cyber data on an additional incident. It is found that there is a significant relationship between total data breach cost and revenue, the total amount of PII, and lawsuits.

Skeoch (2022) presents an economic model for decisions on competing for cybersecurity and cyber insurance investment based on the Gordon-Loeb model. It is found that when the insurance premium is below a certain value, utility is maximized with insurance and security investment.

Strupczewski (2019) uses extreme value theory to model cyber losses due to extreme cyber events. Via a statistical analysis of the SAS OpRisk Global Database, it is found that the Generalized Pareto Distribution method is superior and the best for modeling extreme cyber risks.

Sun et al. (2021) proposes a novel frequency-severity model to analyze hacking breach risks at the company level. A non-parametric generalized Pareto distribution model was used to analyze the Chronology of Data Breaches dataset provided by the Privacy Rights Clearinghouse (PRC) breach frequency and severity. It is found that breach frequency can be modeled by a hurdle Poisson model, and breach severity shows a heavy tail.

Uuganbayar et al. (2019) propose a solution for optimal security investments where cyber insurance is possible by applying time-to-compromise metrics to cyber algorithms. It is found that the best set of countermeasures describes the maximum number of vulnerabilities and increases the required time to compromise a system.

Vakilinia & Sengupta (2019) proposes a synergistic insurance system framework for which organizations collaboratively insure a common platform versus merely themselves. By presenting three models, this study finds that in cooperating on cyber investments and information sharing, organizations are more motivated to invest in cyber insurance.

Wang (2019) presents analytical models for optimizing a firm's cybersecurity spending and cyber insurance based on the effectiveness of spending in reducing cyber threats, vulnerability, and impact. The paper concludes on customizing cyber insurance for firms with itemized threat-specific coverage with a portion of the premium used to help clients with risk knowledge and nudge clients in implementing risk mitigation measures.

Wang & Franke (2020) present an economic model based on a baseline probability model of Poisson arrival frequency with lognormal downtime duration for analyzing enterprise IT service downtime cost. Using a case study, it is found that the total enterprise resources in a single entity can be allocated effectively based on the frequency and duration of the outages.

Woods et al. (2021) propose a method to extract information from insurance prices while accounting for market distortions by conducting a market analysis of the System for Electronic Rate & Form Filing (SERFF) cyber insurance filing provided by NAIC. Using polynomial distributions of the dataset, it is found that prices fall as more insurers begin offering cyber insurance.

Xie et al. (2020) examines the determinants of cyber insurance participation, the amount of coverage offered, and the performance of current cyber insurers via regression analyses of the Cybersecurity and Identity Theft Coverage Supplement dataset created by NAIC. It is found that insurers offer cyber insurance to capitalize on their competitive advantage hypothesis but only somewhat support the business growth hypothesis.

Yang et al. (2019b) proposes a user risk probability model under the condition of interdependent security and correlated risks. Through optimal contract models and analysis of the influence of cyber-insurance on users' self-defense investment, a guide for creating insurance products is created.

Young et al. (2016) presents a framework that incorporates operating principles of the insurance industry to provide quantitative estimates of cyber risk. It highlights optimization techniques toward levels of investment in cybersecurity and insurance for CI.

Zhang & Zhu (2021) present the correlations and dynamics of the cyber risks as well as the users' decisions on the protections with the Markov decision processes. The study demonstrated that the user has higher cyber risks under insurance due to risk compensation, i.e., the user tends to act more recklessly knowing he is protected.

#### 4.2.7 NON-INTRUSIVE RISK SCORING

Organizations depend on third-party organizations for important operational functions. This dependency also exists for the cyber domains of both organizations. Organizations prefer their partners to have a strong cybersecurity posture to reduce their third-party risks. Organizations can utilize intrusive methods, such as network vulnerability scanning and penetration testing, to assess cyber risks of their own networks.

However, a third party cannot conduct such analyses on the network of another organization without their explicit consent, rather may only request such an analysis to be conducted due to the intrusive nature of the methods. On the other hand, conducting a non-intrusive analysis to assess the cyber risks of another organization does not require any involvement or approval from the subject organization, making it more convenient for the parties who need such insights about any organization. For cyber insurance purposes, insurers need to assess the cyber risks of agents to determine the premium. Non-intrusive risk scoring methods help insurers conduct a risk assessment for other organizations with no or partial (i.e., verbal) involvement from the subject organization.

Non-intrusive methods are based on publicly available information, including technical means, such as checking the subject organization's website for outdated certificates, looking up the subject organization's IP addresses from the botnet registers, and searching the dark web for the availability of any confidential data that belong to the subject organization (Keskin et al., 2021).

Non-intrusive risk scoring is getting more popular in recent years with the increasing number of cyber incidents that originated from a third-party organization because, in the cyber domain, an organization's

network depends on the security of partner organizations' networks. The non-intrusive risk scoring methods are generalizable for a diverse set of organizations since the IT infrastructure that is assessed by non-intrusive methods is similar for different organizations. However, the analysis is needed to be conducted individually for different organizations.

The advantage of non-intrusive risk scoring methods is that anyone can conduct it anytime on any organization, without requiring permission from the subject organization since it is conducted by open-source information. On the other hand, the disadvantage of non-intrusive risk scoring is that it is not intrusive, and there is a limited amount of insight that can be utilized from outside of the organization's network about its vulnerabilities and the possible impact of cyber-attacks.

Multiple companies exist that conduct third-party risk scoring, including Security Scorecard, BitSight, FICO, Interos, and ComplyScore. Keskin et al. (2021) conducted a comparative study on the risk scoring methods of such companies to assess their reliability and consistency. Their results suggest that there are similarities in various approaches; however, the scores do not completely converge. The factors considered for the risk scoring assessment include expired website certificates, poor web headers, the number of devices with unsecured open ports, data from the open Web and dark Web regarding the company, compliance with industry standards, response time for patching, and susceptibility to social engineering attacks.

Auditing and questionnaire methods are examples of approaches that require only partial involvement from the agent. Bogomolnii (2017) provided a questionnaire method that employs the critical controls of the Center for Internet Security (CIS) to help insurers during the underwriting process. Other underwriting factors include underwriting meetings, turnover and industry of the insured, and desk research (ENISA, 2017). Auditing based on a framework or industry standard can also help assess risks (NIST, 2020; Tracy, 2019). Mostly used approaches are client meetings, long underwriting questionnaires, and short underwriting questionnaires (Drouin, 2004). The analyses are mostly conducted in conjunction with a relevant risk assessment standard, such as Payment Card Industry Data Security Standard, data privacy standards (General Data Protection Regulation in Europe, Health Insurance Portability and Accountability Act in the U.S.), ISO 27001, and NIST Risk Management Framework (ENISA, 2017).

#### 4.2.8 AI & MACHINE LEARNING

Artificial Intelligence (AI) is defined as “the science and engineering of making intelligent machines, especially intelligent computer programs” (McCarthy, 2004). Machine learning is a branch of AI and “focuses on the use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy” (IBM Cloud Education, 2020). The pros and cons of AI and machine learning are similar to statistical analysis due to the dependence on data. Although AI and machine learning are in their early stages for the cyber insurance sector use cases, some studies utilize such methods in network analysis.

Aditya et al. (2018) presents RiskWriter, a framework to assess the security posture of an entity using both external and business data. Using machine learning HDB-SCAN clustering and random forest classifiers, RiskWriter assesses the internal security posture of over 200,000 firms with high precision and stability across a period of one year. The creation of RiskWriter is limited by the finite data available.

Liu (2019) provided a data analytics tool to quantify cyber risks and predict data breaches by scanning data from the internet and applying deep learning techniques to characterize internet hosts. This provides a numerical and lightweight representation of hosts on the internet. This method provides the ability to detect and predict malicious hosts. The author sees the potential for a paradigm shift in cyber insurance design with this framework.

Lloyd's (2019b) report on artificial intelligence (AI) provides insights into the aspects of AI from the insurance industry perspective. Implications of AI in the insurance sector are manifold: product liability where AI is a part of the production, insurance for self-driving cars, social engineering attacks that leverages AI technologies, misuse of AI in the political domain, and using AI to improve insurance processes. The report provides a comprehensive summary of various aspects of AI.

Pal et al. (2019) comment on the drawbacks of the existing AI-based Bayesian network (BN) cyber vulnerability analysis (C-VA) model proposed in Mukhopadhyay et al. (2013) to assess cyber-risk in IT firms. The re-tests the AI-based model and presents a tighter estimate of IT cyber-risk in environments of low-risk data availability.

Sharma & Mukhopadhyay (2022a) presents a Feedforward Neural Network-based Cyber-risk Assessment and Mitigation model (FNN-CRAM) based on the opportunity theory of crime, rational choice theory, and risk theory to understand DDoS attacks. This study is one of the first to quantify and mitigate cyber risk for the online gaming community using feedforward neural networks. The presented model follows a Weibull distribution and computes expected loss from a cyber-attack. The study concludes that cyber insurance coupled with self-protection is a strong method for mitigating cyber risks due to DDoS attacks on the online gaming community.

## Section 5: Datasets for Cyber Risk Modeling and Quantification

Data sharing among entities is crucial for the cyber insurance industry and needs to be encouraged due to the lack of historical data in this domain compared to the traditional insurance practices on climate or natural disaster risks (ENISA, 2017). In order to enhance the availability of data for cyber insurance purposes, regulators and supervisors should remove the legislation that impedes cyber incident data sharing, and the organizations should involve in active and voluntary data-sharing initiatives. Moreover, international collaboration should be initiated to have a broader understanding of the cyber risk landscape (OECD, 2020b). The cyber risk landscape is understood by considering the asset landscape, threat landscape, controls landscape, and impact landscape (American Academy of Actuaries & Cyber Risk Task Force of Casualty Practice Council, 2022). The existing datasets for cyber risk practice address these landscapes.

Governments and private organizations have launched various data collection initiatives to address the challenges regarding the lack of historical data on cyber risks. In the review of the literature, we identified two distinct categories of datasets used in actuarial sciences towards cyber insurance: datasets on the impact of cyber incidents and datasets about general cybersecurity. The classification of these datasets aligns with Cremer et al. (2022) and the proposed use of the dataset. Although various studies use some datasets, many are not publicly available. The datasets in the scope of this report are presented in 5.1. Given the limited datasets used in actuarial research, we also present several additional cyber datasets that would prove beneficial in future research in 5.2. It is worth mentioning that private datasets are currently being built by not only large data aggregators but individual insurance companies using data scraping and AI (Shipp, 2019). Such datasets may not be labeled as open-source or paid but may be influencing insurance modeling and pricing. See Appendix D for a breakdown of the relevant and recommended datasets and corresponding information.

### 5.1 DATASETS USED BY ACTUARIAL AND INSURANCE RESEARCH

This section outlines the use of cyber databases in the reviewed studies. The datasets used by the researchers in the scope of this review include both open-source and paid datasets aimed at assessing the impact of cyber incidents or various technical cybersecurity-related network datasets. Cyber insurers use impact datasets as a basis to calculate premiums, determine cyber risks, and evaluate other cyber risks. The impact datasets may present losses or frequency of occurrences of cyber risks. Cyber insurers use impact datasets for various analyses, e.g., as a measure by aggregating the data based on industry or other characteristics. The cybersecurity datasets are useful for insurers to test their insureds' countermeasures or vulnerabilities that exist in their network and systems. Likewise, companies or researchers can use cybersecurity data, including intrusion detection information, to uncover vulnerabilities or as measures to mitigate cyber threats. There were 30 studies that utilized datasets, 14 of which utilized the Chronology of Data Breaches provided by Privacy Rights Clearinghouse (PRC).

Research on how to collect data is also being conducted in the cyber insurance industry, and data schemas, such as Cyber Insurance Exposure Data Schema (Cambridge Centre for Risk Studies, 2020) and Vocabulary for Event Recording and Incident Sharing (*The VERIS Framework*, 2013), and CyberCube data schema (O'Brien et al., 2020) have been developed. Data schema provides a framework for collecting and categorizing useful data for insurance practices.

In this section, the information about the datasets used by the articles in the scope of this report is presented. Some of these datasets are publicly available or available with a fee for interested parties, while some of them are not available to the public.



### 5.1.1 CHRONOLOGY OF DATA BREACHES PROVIDED BY THE PRIVACY RIGHTS CLEARINGHOUSE (PRC)

One of the most frequently used and openly available datasets used by actuarial researchers is the Chronology of Data Breaches provided by the Privacy Rights Clearinghouse (PRC). Since 2005, Privacy Rights Clearinghouse has been collecting personal data breaches. As of 2019, they recorded a total of 8,804 data breaches in the U.S., affecting over 11.5 billion PII records. The PRC dataset distinguishes between the different types of breaches (card, hack, insider, physical, portable device, stationary computer loss, unintended disclosure, unknown) and types of business affected (financial and insurance services, retail/merchant, other businesses, educational institutions, government and military, medical services, nonprofits, and unknown). The main limitation of the PRC dataset is that the data used may be underestimated and does not include financial loss information. The database can be downloaded here: <https://privacyrights.org/data-breaches>.

Of the 30 studies using datasets, 14 studies used the PRC dataset to analyze or model data breaches. Bessy-Roland et al. (2021) utilizes 8,871 data breaches from 2010-2021 to test their proposed multivariate Hawkes framework and to predict cyber-attack frequency. Carfora & Orlando (2019) utilized 6,307 data breaches with corresponding information from January 10, 2005 – December 31, 2018, to test the first to their knowledge of a Value at Risk model. Similarly, Carfora & Orlando (2022) analyzed 4,823 breach incidents between January 1, 2010, and December 31, 2019, to better depict the statistical distributions of data breach frequency and severity. Carfora et al. (2019) utilized 5,724 breaches from January 10, 2005 – December 31, 2017, to distinguish between the insurer and insured perspectives on cyber insurance.

Eling & Jung (2018) analyzed 3,327 data breach observations grouped into 144 monthly observations from January 2005-December 31, 2016, to better determine the dependence structures between different types of cyber losses. Eling and Loperfido (2017) analyzed 2,266 data breaches from January 2005-December 2015 using statistical analyses for the distribution of data breaches. Farkas et al. (2021) utilized 8,298 data breach events from 2005- January 23, 2019, to test a method for cyber claim analysis based on regression trees. Lin et al. (2021) investigated 258 incidents from 2011-2016 to determine how insurance companies should price their premiums and how they can better cater to clients to cover a total loss. Sun et al. (2021) evaluated the data breach information of 1,396 companies from January 10, 2005 – March 31, 2019, to test their model based on hacking breach risks for individual companies. Pal et al. (2021) analyzed 9,015 data breaches from 2017 to analyze the effect of individual heavy-tailed and tail-dependent cyber risks.

Additional studies analyze the PRC in addition to other datasets, including the U.S. Department of Health and Human Services, the ITRC dataset, the SAS OpRisk Global dataset (see Section 5.1.1.2), and an additional incident. The U.S. Department of Health and Human Services dataset is a public database that includes healthcare data breaches from 2009-2020. There are 3,241 data breach incidents reported during the period with corresponding information on the breach and those affected. Datasets maintained by the U.S. Department of Health and Human Services can be found here:

<https://catalog.data.gov/organization/hhs-gov>. Liu et al. (2022) used two datasets, including the PRC dataset and the U.S. Department of Health and Human Services dataset, including 9,015 records from the PRC and 3,241 from the Department of Health from 2009-2020 to co-model incidences from various data breaches via a vine copula structure. The ITRC database includes heterogeneous data from over 600 datasets for critical infrastructure modeling and research. The database presents two models to access the datasets. Information on the dataset can be found here: <https://www.itrc.org.uk/themes/databases/>. Xu & Zhang (2021) used the PRC dataset and ITRC dataset from 2019 to investigate data breach catastrophic bonds. Poyraz et al. (2020) utilized two datasets, including the PRC dataset and one additional well-documented incident, to better understand the PII that is stolen, the costs incurred, and the financial impact of a breach. Through analysis, they found 134 data breaches fitting their criteria with full data on 30 of the breaches.

### 5.1.2 SAS® OPRISK GLOBAL DATA

The SAS® OpRisk Global Data is the world's largest and most comprehensive repository of information on publicly reported operational losses over \$100 000, containing more than 37,000 events across all industries worldwide. Along with each loss, the dataset provides information about the company impacted and where the loss occurred. More information on the SAS OpRisk database can be found here: [https://www.sas.com/content/dam/SAS/en\\_us/doc/productbrief/sas-oprisk-global-data-101187.pdf](https://www.sas.com/content/dam/SAS/en_us/doc/productbrief/sas-oprisk-global-data-101187.pdf).

Eling & Wirfs (2019) utilize the PRC dataset with the SAS OpRisk Global dataset to determine the losses from data breaches. The study seeks to understand how various actuarial models across other loss categories can be applied to cyber risks, using 3,327 data breaches from the PRC dataset and 1,579 actual losses from cyber risks from the PRC dataset. Similarly, Eling & Jung (2022) utilize the 2,852 cyber loss observations from the SAS OpRisk Global Dataset from 1984- 2021 to test the Tweedie model and estimate cyber losses faced by the financial industry. Strupczewski (2019) utilized 645 cyber loss observations from the SAS OpRisk Global Dataset to statistically analyze particular loss scenarios.

### 5.1.3 SERFF FILINGS FROM NAIC

The National Association of Insurance Commissioners (NAIC) created the Cybersecurity and Identity Theft Coverage Supplement in 2015, requiring insurance companies to report their financial data on cyber risks; said filings are available in the System for Electronic Rate & Form Filing (SERFF). As of 2016, 49 states and 3,900 insurance companies and filers report their financial information to the SERFF system.

Xie et al. (2020) collected 6,458 firm-year observations from SERFF filings that included U.S. insurance company financial data from 2014-2017 to understand the factors on the insurers offering cyber insurance and that affect the participation in the cyber insurance market. Romanosky et al. (2019) collected 235 filing dockets on U.S. firm cyber insurance policies from 2007-2017 from SERFF filings to determine the losses that were and were not covered, how insurers assess risk, and the factors that help in determining cyber premiums. Woods et al. (2021) analyzed 26 unique filings which contained insurance rate schedules for California, U.S., from the SERFF filings to better understand insurance pricing and market distortions.

### 5.1.4 ISTR REPORT FROM SYMANTEC

The Internet Security Threat Report (ISTR) by Symantec Corporation is a publicly available report that is released every year that contains comprehensive data from millions of attack sensors for mobile protection. The report presents a vulnerability database that provides a large amount of mobile malicious application data. More information on the ISTR report and corresponding information can be found here: <https://www.broadcom.com/support/security-center>. Wang et al. (2021) utilized the 2018 ISTR Report by Symantec to identify global threats in mobile applications, analyzing five of the most prevalent malicious applications for mobile devices in 2017.

### 5.1.5 THOMAS REUTERS EIKON

Thomas Reuters Eikon collects data on over 570 U.S. companies, with many banking and insurance companies, which includes firm information and market capitalization. This dataset has been around for over seven years. Gatzert & Schubert (2022) collected data from all U.S. banking and insurance firms from Thomson Reuters Eikon with a reported market capitalization from 2011-2018 to create a cyber risk consciousness scoring scheme. Through their criteria selection, they chose 124 firms representing the insurance and banking industry to conduct text mining and logistic regression to determine the awareness of cyber risks over the time period.

Other comprehensive datasets which are not publicly available but can be bought by an insurer are the Advisen Cyber Database and Data Breaches from Cowbell Cyber Inc.

### 5.1.6 ADVISEN'S CYBER DATABASE

Advisen's Cyber Database is a proprietary relational database that provides information on cyber risk events that are attributed to financial loss. This database includes more than 90,000 cyber cases involving billions of incidents that affected entities or systems. Access to the cyber loss data can be inquired about here: <https://www.advisenltd.com/data/cyber-loss-data/>. Palsson et al. (2020) presents an analysis of cyber impacts based on the analysis of 75,000 global cyber losses from 2000 to 2018 provided by the Advisen cyber loss dataset.

### 5.1.7 COWBELL CYBER INC. CYBER DATA

Cowbell Cyber Inc. is a company that provides firms evaluations of risk factors for assessing potential cyber exposure. They offer both paid solutions as well as publicly available data reports on emerging cyber risks and the cost of cyber incidents. The challenge with the Cowbell Cyber Inc. dataset is that it does not provide information on the size of the data breach or firm-specific factors that can drive the financial costs of events. Access to Cowbell Cyber Inc's resources, including data reports and specified data and information for policyholders, insurers, and industries can be found here: <https://cowbell.insure/resources/>.

Eling et al. (2022) utilizes 933 cyber breach records from Cowbell Cyber Inc. collected from U.S. firms and public and private entities from 1992 to 2019 to identify firm-specific factors which interact with the cost of a breach. Likewise, Jung et al. (2021) utilized Cowbell Cyber, one of the largest databases for data breach losses, analyzing 21,555 cyber loss observations from 2005-2018 and comparing them to the PRC dataset to determine the size of the next large data breach loss.

### 5.1.8 PRIVATE/PROPRIETARY DATASETS

Others used various datasets that were not publicly available to understand the impact of cyber events. Given they are not openly available to the public, we just will briefly mention them for potential future reference. Carannante et al. (2022) utilize Italian market cyber loss data from Accenture, although they do not provide additional information on the dataset. Sharma and Mukhopadhyay (2022a) utilize a dataset of 10,329 distributed denial of service (DDoS) attacks in the MMOG (online gaming) industry captured by CDN, collected from 2012-2018.

Mukhopadhyay et al. (2019) utilized a CSI-FBI survey (1997-2010), although they provided no additional data information. Pal et al. (2019) used log data of four perimeter security elements, that is, Security Policy Failure (SPF), Firewall (FW), Antivirus (AV), and Security Elements Failure (SEF), from the information technology and services (ITS) departments of both the Indian Institute of Management Calcutta (IIMC) and the University of Southern California (USC) for 2 years. Watson et al. (2022) interviewed ten New Jersey banking officials from CISO or other organizations from banks listed on the State of New Jersey Department of Banking and Insurance public website and collected subsequent data.

Acharya et al. (2021) used power grid and commercial EVCS data from Manhattan, New York, to perform a case study. Aditya et al. (2018) utilized Security Scorecard, which provided over 200,000 records of external or business cyber incident logs and vendor data for a period of 12 months. Pate-Cornell & Kuypers (2021) collected 60,000 cyber incident records from SpaceCorp.

## 5.2 ADDITIONAL CYBER-RISK-RELATED DATASETS

While several cyber datasets were utilized in the cyber insurance or actuarial science research in this review, there are a host of cyber databases not covered in the research that can be used to help in modeling or pricing cyber insurance.

### 5.2.1 CYBER ACUVIEW

Cyber AcuView is a company aimed at helping industry stakeholders with cyber risk mitigation and ensuring a competitive cyber insurance market. They compile and analyze cyber-related data to enhance value and service. Cyber AcuView offers services including industry data collection and analysis, cyber industry data information standards, regulator and government agency collaboration, law enforcement and security agency coordination, and systemic risk evaluation. Through analyses of cyber trends and collecting data from the industry, they provide insights on attacks and the causes of data loss. A list of their services can be found here: <https://cyberacuvview.com/services/>.

### 5.2.2 DATALOSSDB

DataLossDB is a database aimed at documenting and reporting data loss incidents from around the world and is maintained by Risk Based Security (formerly Open Security Foundation). The data collected focuses on breaches of PII that are lost or stolen by third parties. Data losses are acquired from verifiable databases and government resources. As of June 4, 2008, DataLossDB contained more than 1,000 breaches of PII, which include over 330 million records. More information on DataLossDB can be found here: [http://datalosssdb.org/primary\\_sources](http://datalosssdb.org/primary_sources).

### 5.2.3 DHS IMPACT

The DHS Information Marketplace for Policy and Analysis of Cyber Risk and Trust (IMPACT) repository aims to support global cyber risk research by presenting and developing real-world data and information-sharing capabilities between industry, government, and academia. IMPACT aims to provide a more open marketplace to connect and socialize, policy and analysis are driven by and for real-world issues, and refining cyber risk and trust, so information is deemed critical infrastructure, beyond defense and threats. IMPACT is the only freely available, legally collected, and distributed repository of large-scale cybersecurity data and analytical tools.

The IMPACT community includes data providers, data hosts, cybersecurity researchers, and more that provide, host, use and benefit from the high-quality cyber datasets. The repository continually seeks to add new data to respond to cyber risk management research and trends to ensure timely and high-value research. The IMPACT model also tests various data-sharing models for use in research and development. IMPACT's main purpose is to facilitate data sharing, which consists of metadata discovery (FIND), data and tool matchmaking (GET & USE), a social feedback loop (FORUM), and a rules broker that enables the other components.

The IMPACT repository includes cyber datasets, tools, third-party datasets, and third-party tools spanning from 2015-2022 from a variety of academic, government, and industry sources, including the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS CISA), Carnegie Mellon University, and Parsons Inc. The datasets available through this repository include unrestricted data (commercial and noncommercial use), quasi-restricted data (commercial and noncommercial use if approved by the Data Provider), and restricted data (require an MOA to use).

Here is a link to the Impact database: <https://www.impactcybertrust.org/>.

#### 5.2.4 NETDILIGENCE

NetDiligence is a provider of cyber risk management software and services in the insurance industry. Since 2011, they have published a Cyber Claims Study and now offer a proprietary eRiskHub that analyzes the severity, frequency, and data exposure for particular claims. In the 2020 Cyber Claims Study, the report discusses incidents that occurred between 2015-2019, analyzing 3,547 claims. The 2022 Cyber Claims Study can be found here: [https://netdiligence.com/wp-content/uploads/2021/03/NetD\\_2020\\_Claims\\_Study\\_1.2.pdf](https://netdiligence.com/wp-content/uploads/2021/03/NetD_2020_Claims_Study_1.2.pdf)

#### 5.2.5 FBI INTERNET CRIME COMPLAINT CENTER REPORT

The FBI Internet Crime Complaint Center (IC3) has been producing annual cybercrime reports since 2000. It provides aggregated frequency and severity of internet-related crimes in the U.S. and abroad. The annual reports and subsequent data can be found here: <https://www.ic3.gov/Home/AnnualReports>.

#### 5.2.6 ISO VERISK

ISO is a Verisk Analytics business that provides an array of commercial and personal insurance offerings, serving insurers, reinsurers, agents, regulators, risk managers, and other members of the insurance marketplace. The ISO Verisk cyber insurance program has collected premium, exposure, and loss data for cyber liability and first-party coverages between 2010 and 2014 and insights on over 100 million organizations. The Verisk services offer a host of data services to help in operations and compliance. More information on the Verisk program can be found here: <https://www.verisk.com/insurance/products/cyber-insurance-program/>.

#### 5.2.6 ORX OPERATIONAL RISK DATA

The ORX Operational Risk Dataset provides an analysis and trend forecast of operational risk losses from 2015-2020. Two reports are produced each year – one for the insurance sector and the other for the backing sector. The reports include a comprehensive analysis of global operational risk loss data, including loss frequency and severity from 2015-2020, event frequency and the total loss by business and event, losses by business type, geographic breakdown of the losses, and risk in focus to highlight the impact of COVID-19 on operational risks. Each report costs ~\$930. The report purchase requests can be found here: <https://engage.orx.org/buy/annual-loss-reports>.

#### 5.2.7 PONEMON INSTITUTE COST OF DATA BREACH STUDY

Ponemon Institute produces an annual survey report on the cost of data breaches, using aggregate severity and frequency information. The Ponemon Library offers several reports with data on security incidents from around the world. A repository of these resources can be found here: <https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf>.

#### 5.2.8 VERIS COMMUNITY DATABASE (VCDB)

The VERIS Community Database (VCDB) is an offshoot of the annual Verizon Data Breach Investigation Report (DBIR) which seeks to improve information sharing of cybersecurity incidents to support research and practices. Since 2008, this database has captured publicly disclosed security incidents, including data breaches and aggregate frequency data in raw format to help improve data manipulation. This database can be found here: <http://veriscommunity.net/vcdb.html>.

### 5.2.9 COMMON VULNERABILITIES AND EXPOSURES (CVE)

The Common Vulnerabilities and Exposures (CVE) is a cyber database maintained by the Industry Consortium for Advancement of Security on the Internet (ICASI). The dataset includes vulnerability and exposure information on the common cyber threats to entities. The dataset and corresponding information can be found here: <https://cve.mitre.org/cve/cvrf.html>.

### 5.2.10 COMMON VULNERABILITY SCORING SYSTEM (CVSS)

The Common Vulnerability Scoring System (CVSS) is an open framework maintained by FIRST for communicating the characteristics and severity of software vulnerabilities. The open-source vulnerability system and applicable information can be found here: <https://nvd.nist.gov/vuln-metrics/cvss>.

### 5.2.11 HONEYPOT DATA

Honeypots provide information about vulnerable systems and insights into malicious attack activities. The Leurre.com honeypot project provides information on dozens of honeypot sensors placed globally, which can be used as event series to determine frequency distributions. Likewise, the HoneyNet project seeks to investigate the latest attacks and develop open-source security tools aimed at improving internet security. This project conducts data analyses, conducts security tool development, and collects data on attackers and malicious systems used. Many of the tools or services, including Greedybear, T-POT, and Intel Owl, are open-source and available via GitHub. More information and access to the HoneyNet Project can be found here: <https://www.honeynet.org/projects/>.

## Section 6: Challenges

Through the review analysis, we identified several challenges that limit actuarial work in cyber insurance. The identified challenges include a lack of cyber data, information asymmetry, correlated risk/ losses, cybersecurity interdependence, and quantification of cyber risk.

### 6.1 INADEQUATE DATA

One of the most cited challenges of creating or pricing cyber insurance is inadequate cyber data and limited availability (ENISA, 2012; CISA, 2019). Cyber risk “refers to a multitude of different sources of risk affecting the information and technology assets of a firm” (Biener et al., 2015, p. 2). Yet, cyber event and loss data is limited and is often not available in the desired amount or size. As systems continuously evolve, cyber threats are becoming increasingly sophisticated and challenging. Many studies cite the lack of historical data but given the fluid nature of cyber threats and attack methods, historical data may not be pertinent to the next attack. Cyber risks face a fast-paced evolution that is hard to quantify with historical data creating additional challenges for the insurer.

Inadequate data is specific to cyber insurance, as traditional insurance offerings like auto insurance include large sets of historical data. Those interested in offering auto insurance may subscribe to one of many datasets and design and price premiums accordingly. For cyber insurance, there is not a widely accepted dataset that can accurately and efficiently help design or price cyber premiums.

### 6.2 INFORMATION ASYMMETRY

An additional challenge within cyber insurance is information asymmetry. Cyber threats are evolving dynamically in a particularly non-stationary risk landscape. For cyber threats, there is an asymmetric relationship between cyber threats and cyber defense. In this, an attacker only needs to know how to successfully attack one vulnerability, while the defender needs to defend every vulnerability. This is a win-lose battle, where attackers outnumber defenders and in no way is one able to fully defend a system from potential threats. It is in this landscape that information asymmetry arises where one party knows more than another, which is the reality of the information age we live in. Within this the interrelated nature of information systems makes it difficult to uncover the causes of data losses and the identity of attackers, increasing an entity's reluctance to invest in protection or transfer their risk via cyber insurance (Biener et al., 2015).

Unlike other insurance fields, cyber risks are constantly changing, so being insured or “protected” from threats does not necessarily mitigate the risks, as new vulnerabilities can constantly be exploited. For example, with auto insurance, drivers may opt to take a defensive driving course to lower their insurance premium, making them more equipped to handle themselves on the road, yet cyber training is only as good as the known risks (i.e., full system vulnerabilities and human error cannot be accounted for).

### 6.3 CORRELATED AND INTERDEPENDENT RISKS

Additional challenges in cyber insurance arise due to correlated or interdependent risks. Cyber interdependency is a state in which aggregate cyber risks arise due to common interconnections that cannot be captured. Likewise, correlation among risks hinders efficient pooling as it does not fully account for the randomness of loss occurrence (Biener et al., 2015). This phenomenon of correlated and interdependent risks can cause the cyber insurance market to be both underdeveloped and underused (Dou et al., 2020) leading the insurers to a challenging portfolio management landscape (Coburn et al., 2019). Bohme et al. (2006) discuss how cyber insurance is for those risks that have high internal and low global correlations.

#### 6.4 QUANTIFICATION OF CYBER RISK

In the literature, several researchers and practitioners cite pricing or creating cyber insurance policies as a challenge due to the inability to quantify cyber risks (CISA, 2019; Mukhopadhyay et al., 2019). Although several models to quantify IT risk exists (i.e., CRAMM and VFA), the changing nature of cyber threats and limited historical data limit the ability to fully quantify them. In order to properly mitigate cyber risks, being able to model the trends and cyber vulnerabilities, threats, and risks is critical. According to Kenneally et al. (2018), a “challenge to more accurate and complete risk understanding is accumulating risk measures inside the firm and correlating these with externally-facing risk data and with actual loss event data” (pg. 3). The ability to quantify cyber risks relies on adequate data and a better understanding of information asymmetry and correlated risks, which are challenges unique to cyber insurance.



## Section 7: Knowledge Gaps & Future Research

We identified several knowledge gaps and future research topics in this literature analysis. Table 2 presents an overview of the main knowledge gaps and areas for future research related to cyber insurance modeling and pricing, data, and cyber risk management as a whole. Building on Tondel et al. (2016), studies highlight the need for more research on several topics related to risk management, security economics, and business modeling. Within this, there are significant gaps in understanding and measuring risk and associated costs toward designing and pricing cyber insurance, as well as aiding in the decision-making of the insurer or insured (Eling et al., 2021). Cyber insurance actors would benefit from research in these various fields, where a better understanding of pricing models, product design, and datasets used will help build a stronger foundation for cyber insurance offerings. Here, research calls for greater collaboration between stakeholders and empirical research that goes beyond scenario analyses to include data generation and interdisciplinary qualitative dialogue (Eling et al., 2021; Marotta & McShane, 2018). Within cyber insurance research, several challenges exist (see Section 6) that emphasize the knowledge gaps and lead to additional research avenues.

As presented in Table 2, there is a need for improved models, methods, and datasets related to cyber insurance. Due to the lack of actuarial cyber data, there is an increased need for cyber datasets that are not only comprehensive but provide real-time information that is openly available. Additional research is warranted to determine the trends and profitability of the cyber insurance industry as more data becomes available and losses are experienced across sectors (Cole & Fier, 2021). Potential future research can also include an analysis of the effect of cybersecurity risk management and insurance spending on the market value loss of attacked entities (McShane & Nguyen, 2020). The results of many of the event studies, including McShane and Nguyen's (2020), can be used in cyber insurance price modeling while accounting for the challenges discussed in Section 6.

The research also emphasizes the need for more qualitative empirical research using said datasets to understand and offer more comprehensive cyber insurance. As presented in Section 4, several research methods exist in cyber insurance research, yet a majority are quantitative. There is a call for more qualitative cybersecurity research which uses interviews, focus groups, or conduct case studies that combine several techniques (Fujs et al., 2019), including the cyber insurance industry. In this, risk ratings and current exposure and risk categorizations should be qualitatively analyzed to determine existing correlations and methods for operationalization (Innerhofer-Oberperfler & Breu, 2010). Marotta and McShane, suggest surveys and discussions with experts on honeypot usage in the corporate and government environments (2018).

Likewise, studies suggest future research in the under-researched area of cyber reinsurance. In this, studies suggest discussing whether cyber reinsurance exists and subsequent challenges (Jung, 2021; Pooser et al., 2018). Additionally, research is sought in determining capital market alternatives to traditional cyber reinsurance, including the use of CAT bonds, parametric insurance, catastrophic risk exchange, and insurance-linked securities (Liu et al., 2021; Xu & Zhang, 2021). For example, Xu and Zhang (2021) recommend investigating the use of CAT bonds as an alternative to traditional cyber reinsurance for other cyber risks that cause significant monetary loss including worm infection and distributed denial-of-service (DDoS) attacks.

**Table 2**  
**KNOWLEDGE GAPS AND FUTURE RESEARCH**

Knowledge Gap	Questions
<b>Cyber Insurance Design &amp; Pricing</b>	<p>What metrics are most useful for evaluating cyber-risk and cost?</p> <p>How can the actuarial sector arrive at a widely accepted data set for managing and pricing cyber insurance?</p> <p>What information are enterprises willing to provide to an insurance company to obtain a cheaper premium or to obtain insurance?</p> <p>How can cyber risk insurance be regulated? Are new regulatory models needed for cyber risks? How can risk dwelling in insurance policies be reduced and offer fuller coverage with fewer sub-limits and exclusions desired by policyholders?</p> <p>What are the differences between models for admitted versus non-admitted (i.e., excess and surplus line) insurers?</p> <p>How can insurance companies view cyber risk as an operational risk and link it to underwriting?</p> <p>What would be the impact of catastrophic cyber risk events on cyber insurance market?</p> <p>How reliable are the available third-part risk rating solutions?</p> <p>What are the challenges with reinsurance of cyber risks?</p> <p>Do capital market alternatives (i.e., CAT bonds, parametric insurance, catastrophic risk exchange, insurance-linked securities) for traditional cyber reinsurance exist? If so, how can these alternatives be used in cyber risk transfer?</p> <p>Is cyber insurance a profitable line of business?</p> <p>What are the effects of different pricing strategies on the development of the cybersecurity marketplace?</p> <p>How can risk scores be developed using Bayesian probabilities to assess cyber risk?</p>
<b>Cyber Data</b>	<p>How are public/ private information sharing platforms designed to aid in the availability and quality of cyber risk data?</p> <p>How can scenarios be used as an alternative to dealing with the lack of cyber data?</p> <p>How can methods for collecting and analyzing measurement data be improved to reduce measurement costs and increase reliability?</p> <p>How does the risk of change affect cyber risk data sets? Would behavioral economics be useful in helping determine the motivations of attacks?</p> <p>How can the collection of cyber data be improved to account for changes in the internal and external environment? How can one effectively manage cyber risks toward building cyber resilience?</p>

Knowledge Gap	Questions
<b>Cyber Risk Management</b>	<p>How does cyber-insurance influence the security of organizations, positively and negatively?</p> <p>How do organizations make decisions to purchase (or not purchase) cyber insurance?</p> <p>Will businesses implement security improvements to obtain cheaper premiums rather than simply rely on cyber insurance alone? How can insurance companies act to reduce moral hazards?</p> <p>How can one expand cybersecurity offerings and data, to improve not only technical data solutions but a greater understanding of the socioeconomic risk factors, processes, and people in cybersecurity?</p> <p>How can cyber risks and corresponding decisions be promoted among upper management for a more holistic cyber decision-making approach and corporate governance?</p> <p>What are the differences between cyber risk terminology and frameworks? How can a better understanding of these differences aid in cyber risk management?</p> <p>How will risk transfer work for extreme cyber risks?</p> <p>How can a global dialogue be created to account for systemic or catastrophic cyber risks in cyber insurance or underwriting?</p> <p>What are other determinants of cybersecurity breach likelihood?</p> <p>What impacts do cyberattacks have on business operations outside of firm value?</p> <p>How does the trade-off between coverage and efficiency regarding the formulation of a remediation strategy safeguard against cyber vulnerabilities?</p> <p>How do cyberattacks impact geographical regions outside of the United States? How can conducting cyber risk analysis in other geographical regions highlight the potential effects of cultural differences and legal origins on how market participants respond to cyberattacks?</p> <p>Does a correlation exist between cyber risks and other types of risks (e.g., geopolitical risks, global health crises)?</p> <p>Will conducting interdisciplinary studies help understand cyber risk management and cyber insurance practices?</p> <p>How can cyber risks and transfer strategies be developed and implemented to promote resiliency? How can creating a cyber-resilient management framework help organizations and governments adapt to changes in the cyber environment?</p>



**Give us your feedback!**

Take a short survey on this report.

[Click Here](#)

**SOA**  
Research  
INSTITUTE

## Section 8: Acknowledgments

The researchers' deepest gratitude goes to those without whose efforts this project could not have come to fruition: the General Insurance Research Committee of the Society of Actuaries Research Institute for funding the research, external reviewers for their diligent work reviewing and editing this report for accuracy and relevance, and Project Oversight Group for overseeing the resource gathering, analyzing and discussing literature findings.

External Reviewers:

Michael McShane, Professor, Old Dominion University

C. Ariel Pinto, Professor, Old Dominion University

Project Oversight Group at the Society of Actuaries:

R. Dale Hall, FSA, MAAA, CFA, CERA, Managing Director of Research

Robert Montgomery, ASA, MAAA, Research Project Manager

Any opinions expressed may not reflect their opinions nor those of their employers. Any errors belong to the authors alone.

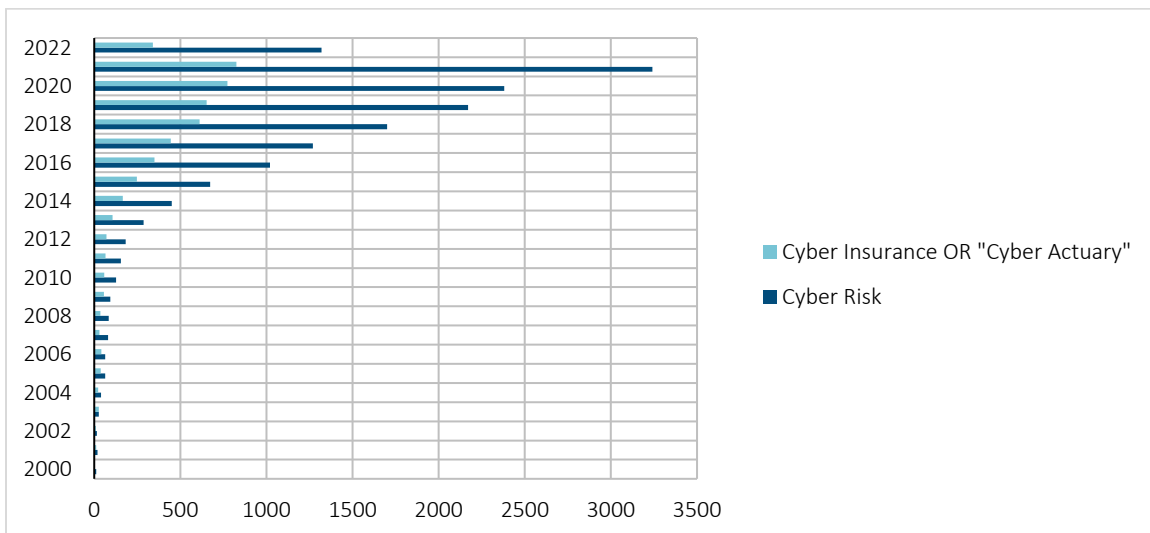
## Appendices

### APPENDIX A: GOOGLE SCHOLAR CITATIONS

**Table 3**  
GOOGLE SCHOLAR CITATIONS AS OF JUNE 7, 2022

Year	"Cyber Risk"	"Cyber Insurance" OR "Cyber Actuary"
2000	12	3
2001	19	11
2002	15	10
2003	27	27
2004	40	22
2005	63	38
2006	64	41
2007	81	31
2008	85	36
2009	93	56
2010	127	58
2011	155	66
2012	183	71
2013	286	106
2014	451	165
2015	673	247
2016	1,020	349
2017	1,270	444
2018	1,700	612
2019	2,170	653
2020	2,380	774
2021	3,240	825
2022	1,250	325

**Figure 11**  
GOOGLE SCHOLAR CITATIONS AS OF JUNE 17, 2022



## APPENDIX B: COMPENDIUM OF GREY LITERATURE

Year	Author/Organization	Title	Category	URL
2020	Advisen and PartnerRe	Cyber Insurance - The Market's View	Market	<a href="https://library.cyentia.com/report/report_005654.html">https://library.cyentia.com/report/report_005654.html</a>
2020	Advisen and Zurich	Information Security and Cyber Risk Management Report 2020	Market	<a href="https://library.cyentia.com/report/report_006084.html">https://library.cyentia.com/report/report_006084.html</a>
2016	Aite Novarica	Cyber Insurance and Cybersecurity	Market	<a href="https://library.cyentia.com/report/report_001099.html">https://library.cyentia.com/report/report_001099.html</a>
2022	American Academy of Actuaries and Cyber Risk Task Force, Casualty Practice Council	Cyber Risk Toolkit	Datasets	<a href="https://www.actuary.org/sites/default/files/2022-02/CyberRiskToolkit.Feb22.pdf">https://www.actuary.org/sites/default/files/2022-02/CyberRiskToolkit.Feb22.pdf</a>
2021	Aon	Aon's E&O   Cyber Insurance Snapshot	Market	<a href="https://library.cyentia.com/report/report_007172.html">https://library.cyentia.com/report/report_007172.html</a>
2021	Aon	U.S. Cyber Market Update	Market	<a href="http://thoughtleadership.aon.com/Documents/20210609-2021-cyber-market-update.pdf">http://thoughtleadership.aon.com/Documents/20210609-2021-cyber-market-update.pdf</a>
2020	Bean	Exposure Measures for Pricing and Analyzing the Risks in Cyber Insurance	Coverage	<a href="https://www.soa.org/49f336/globalassets/assets/files/resources/research-report/2020/exposure-measures-cyber-insurance.pdf">https://www.soa.org/49f336/globalassets/assets/files/resources/research-report/2020/exposure-measures-cyber-insurance.pdf</a>
2017	Bogomolnii	Cyber Insurance Conundrum: Using CIS Critical Security Controls for Underwriting Cyber Risk- A Masters Degree Candidate Presentation	Model	<a href="https://www.sans.org/webcasts/cyber-insurance-conundrum-cis-critical-security-controls-underwriting-cyber-risk-masters-degree-candidate-presentation-107015/">https://www.sans.org/webcasts/cyber-insurance-conundrum-cis-critical-security-controls-underwriting-cyber-risk-masters-degree-candidate-presentation-107015/</a>
2020	Cambridge Centre for Risk Studies	Cyber Insurance Exposure Data Schema V1.0	Data Schema	<a href="https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-data-schema-v1.0.pdf">https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-data-schema-v1.0.pdf</a>
2019	Cambridge Centre for Risk Studies	Risk Management for the Consumer Sectors	Case Study	<a href="https://www.jbs.cam.ac.uk/wp-content/uploads/2021/11/crs-risk-management-for-the-consumer-sectors.pdf">https://www.jbs.cam.ac.uk/wp-content/uploads/2021/11/crs-risk-management-for-the-consumer-sectors.pdf</a>
2018	Cambridge Centre for Risk Studies	Global Risk Index 2019 Executive Summary	Market	<a href="https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-global-risk-index-exec-summary-2019.pdf">https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-global-risk-index-exec-summary-2019.pdf</a>
2017	Cambridge Centre for Risk Studies	2017 Cyber Risk Landscape	Market	<a href="https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-rms-cyber-risk-landscape-2017.pdf">https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-rms-cyber-risk-landscape-2017.pdf</a>
2022	Carter, Pain and Enoizi	Insuring Hostile Cyber Activity: In Search of Sustainable Solutions	Market	<a href="https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cybersolutions_web.pdf">https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cybersolutions_web.pdf</a>
2019	CISA	Assessment of the Cyber Insurance Market	Market	<a href="https://www.cisa.gov/sites/default/files/publications/19_1115_cisa_OCE-Cyber-Insurance-Market-Assessment.pdf">https://www.cisa.gov/sites/default/files/publications/19_1115_cisa_OCE-Cyber-Insurance-Market-Assessment.pdf</a>
2014	CISA	Insurance Industry Working Session Readout Report	Challenges	<a href="https://www.cisa.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf">https://www.cisa.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf</a>
2014	CISA	Cyber Insurance Roundtable Readout Report - Health Care and Cyber	Challenges	<a href="https://www.cisa.gov/sites/default/files/publications/February%202014%20Cyber%20Insu">https://www.cisa.gov/sites/default/files/publications/February%202014%20Cyber%20Insu</a>

Year	Author/Organization	Title	Category	URL
		Risk Management: Cost/Benefit Approaches		<a href="#">rance%20Health%20Care%20Use%20Case%20Roundtable.pdf</a>
2013	CISA	Cyber Risk Culture Roundtable Readout Report	Challenges	<a href="https://www.cisa.gov/sites/default/files/publications/May%202013%20Cyber%20Risk%20Culture%20Roundtable.pdf">https://www.cisa.gov/sites/default/files/publications/May%202013%20Cyber%20Risk%20Culture%20Roundtable.pdf</a>
2012	CISA	Cybersecurity Insurance Workshop Readout Report	Challenges	<a href="https://www.cisa.gov/sites/default/files/publications/November%202012%20Cybersecurity%20Insurance%20Workshop.pdf">https://www.cisa.gov/sites/default/files/publications/November%202012%20Cybersecurity%20Insurance%20Workshop.pdf</a>
2014	CISA	Cybersecurity Insurance Reports   CISA	Challenges	<a href="https://www.cisa.gov/publication/cybersecurity-insurance-reports">https://www.cisa.gov/publication/cybersecurity-insurance-reports</a>
2021	Citi GPS and Cambridge Centre for Risk Studies	Systemic Risk: Systemic Solutions for an Increasingly Interconnected World	Catastrophic cyber risks	<a href="https://www.jbs.cam.ac.uk/wp-content/uploads/2021/04/crs-citigps-systemic-risks-report.pdf">https://www.jbs.cam.ac.uk/wp-content/uploads/2021/04/crs-citigps-systemic-risks-report.pdf</a>
2021	Coalition	Cyber Insurance Claims Report: H1 2021	Market	<a href="https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2020-09-Coalition-Cyber-Insurance-Claims-Report-2020.pdf">https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2020-09-Coalition-Cyber-Insurance-Claims-Report-2020.pdf</a>
2019	Coburn, Daffron, Quantrill, et al.	Cyber Risk Outlook	Market	<a href="https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-risk-outlook-2019.pdf">https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-risk-outlook-2019.pdf</a>
2018	Coburn, Daffron, Smith, et al.	Cyber Risk Outlook	Market	<a href="https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-risk-outlook-2018.pdf">https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-risk-outlook-2018.pdf</a>
2018	Corax and Clyde&Co	2018 Cyber Breach Insights	Market	<a href="https://library.cyentia.com/report/report_002913.html">https://library.cyentia.com/report/report_002913.html</a>
2022	Corix Partners and Cyber Solace	Cyber Insurance	Market	<a href="https://library.cyentia.com/report/report_008822.html">https://library.cyentia.com/report/report_008822.html</a>
2022	Cowbell Cyber	Cyber Round-Up Q2 2022	Market	<a href="https://cowbell.insure/sme-cyber-round-up/">https://cowbell.insure/sme-cyber-round-up/</a>
2017	Cutler et al.	Cybersecurity: Impact on Insurance Business	Model	<a href="https://www.soa.org/globalassets/assets/files/static-pages/sections/joint-risk-mgmt/cyber-security-impact.pdf">https://www.soa.org/globalassets/assets/files/static-pages/sections/joint-risk-mgmt/cyber-security-impact.pdf</a>
2019	Cyber Risk Insurance Task Force, American Academy of Actuaries Casualty Practice Council	Cyber Risk Insurance: A Resource Guide for Actuaries	Compendium	<a href="https://www.actuary.org/sites/default/files/2019-06/cyber-risk-insurance.pdf">https://www.actuary.org/sites/default/files/2019-06/cyber-risk-insurance.pdf</a>
2004	Drouin	Cyber Risk Insurance	General Summary	<a href="https://www.sans.org/white-papers/1412/">https://www.sans.org/white-papers/1412/</a>
2016	Eling and Schnell	Ten Key Questions on Cyber Risk and Cyber Risk Insurance	Compendium	<a href="https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber-risk-10_key_questions.pdf">https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber-risk-10_key_questions.pdf</a>
2012	ENISA	Incentives and Barriers of the Cyber Insurance Market in Europe	Challenges	<a href="https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe">https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe</a>
2018	European Insurance and Occupational Pensions Authority	Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies	Pricing	<a href="https://data.europa.eu/doi/10.2854/33407">https://data.europa.eu/doi/10.2854/33407</a>
2020	European Insurance and Occupational Pensions Authority	Cyber Risk for Insurers-Challenges and Opportunities	Challenges	<a href="https://doi.org/10.2854/305969">https://doi.org/10.2854/305969</a>

Year	Author/Organization	Title	Category	URL
2020	ENISA	EIOPA Strategy on Cyber Underwriting	Challenges	<a href="https://data.europa.eu/doi/10.2854/793935">https://data.europa.eu/doi/10.2854/793935</a>
2016	ENISA	Cyber Insurance	Market	<a href="https://data.europa.eu/doi/10.2824/065381">https://data.europa.eu/doi/10.2824/065381</a>
2017	ENISA	Commonality of Risk Assessment Language in Cyber Insurance	Challenges	<a href="https://data.europa.eu/doi/10.2824/691163">https://data.europa.eu/doi/10.2824/691163</a>
2020	European Systemic Risk Board	Systemic Cyber Risk	Systemic risks	<a href="https://data.europa.eu/doi/10.2849/566567">https://data.europa.eu/doi/10.2849/566567</a>
2017	Evan et al.	Cyber Terrorism: Assessment of the Threat to Insurance	Systemic risks	<a href="https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/pool-re-cyber-terrorism.pdf">https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/pool-re-cyber-terrorism.pdf</a>
2022	Forscey et al.	Systemic Cyber Risk: A Primer	Systemic risks	<a href="https://carnegieendowment.org/2022/03/07/systemic-cyber-risk-primer-pub-86531">https://carnegieendowment.org/2022/03/07/systemic-cyber-risk-primer-pub-86531</a>
2022	Gallagher Re and Risk Management Solutions, Inc.	An Analytics-Led Approach to Cyber Intelligence	Reinsurance	<a href="https://www.rms.com/sites/default/files/2022-02/RMS-Gallagher-Case-Study-Feb2022.pdf">https://www.rms.com/sites/default/files/2022-02/RMS-Gallagher-Case-Study-Feb2022.pdf</a>
2020	Hall	Exposure Measures for Pricing and Analyzing the Risks in Cyber Insurance Podcast	Model	<a href="https://www.soa.org/resources/research-reports/2020/exposure-measures-cyber-insurance/">https://www.soa.org/resources/research-reports/2020/exposure-measures-cyber-insurance/</a>
2015	Hartwig and Wilkinson	Cyber Risk: Threat and Opportunity	Market	<a href="https://www.iii.org/sites/default/files/docs/pdf/cyber_risk_wp_final_102015.pdf">https://www.iii.org/sites/default/files/docs/pdf/cyber_risk_wp_final_102015.pdf</a>
2016	Hofmann	Cyber Insurance as a Risk Mitigation Strategy	Insurance as incentive	<a href="https://cams.mit.edu/wp-content/uploads/research_brief_-_contours_of_an_emerging_market_for_cyber_risk_transfer.pdf">https://cams.mit.edu/wp-content/uploads/research_brief_-_contours_of_an_emerging_market_for_cyber_risk_transfer.pdf</a>
2018	Hofmann	Advancing Accumulation Risk Management in Cyber Insurance	Reinsurance	<a href="https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/report_advancing_accumulation_risk_management_in_cyber_insurance.pdf">https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/report_advancing_accumulation_risk_management_in_cyber_insurance.pdf</a>
2021	Howden	Cyber Insurance: A Hard Reset	Market	<a href="https://library.cyentia.com/report/report_008129.html">https://library.cyentia.com/report/report_008129.html</a>
2018	Atluri	Why Cyber Insurance Needs Probabilistic and Statistical Cyber risk Assessments More Than Ever		<a href="https://www.isaca.org/resources/isaca-journal/issues/2018/volume-2/why-cyber-insurance-needs-probabilistic-and-statistical-cyber-risk-assessments-more-than-ever">https://www.isaca.org/resources/isaca-journal/issues/2018/volume-2/why-cyber-insurance-needs-probabilistic-and-statistical-cyber-risk-assessments-more-than-ever</a>
2021	Johansmeyer	Cybersecurity Insurance Has a Big Problem	Challenges	<a href="https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem">https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem</a>
2019	Kaffenberger and Kopp	Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment	Systemic risks	<a href="https://carnegieendowment.org/files/Kaffenberger_Cyber_Risk_Scenarios_final1.pdf">https://carnegieendowment.org/files/Kaffenberger_Cyber_Risk_Scenarios_final1.pdf</a>
2016	Kelly et al.	Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy	Case Study	<a href="https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-integrated-infrastructure-cyber-resiliency-in-society.pdf">https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-integrated-infrastructure-cyber-resiliency-in-society.pdf</a>
2019	Liu	A New Paradigm in Risk-Informed Cyber Insurance Policy Design: Meta-Policies and Risk Aggregation	Model	<a href="https://apps.dtic.mil/sti/pdfs/AD1071891.pdf">https://apps.dtic.mil/sti/pdfs/AD1071891.pdf</a>



Year	Author/Organization	Title	Category	URL
2015	Lloyd's	Business Blackout	Case Study	<a href="https://assets.lloyds.com/assets/pdf-business-blackout-business-blackout20150708/1/pdf-business-blackout-business-blackout20150708.pdf">https://assets.lloyds.com/assets/pdf-business-blackout-business-blackout20150708/1/pdf-business-blackout-business-blackout20150708.pdf</a>
2021	Lloyd's	Cyber Risk in Aviation	Case Study	<a href="https://www.lloyds.com/news-and-insights/risk-reports/library/cyber-risk-in-aviation">https://www.lloyds.com/news-and-insights/risk-reports/library/cyber-risk-in-aviation</a>
2021	Lloyd's	Cyber Risk	Case Study	<a href="https://www.lloyds.com/news-and-insights/risk-reports/library/icsreport">https://www.lloyds.com/news-and-insights/risk-reports/library/icsreport</a>
2020	Lloyd's	Safeguarding Reputation	Case Study	<a href="https://www.lloyds.com/news-and-insights/risk-reports/library/safeguarding-reputation">https://www.lloyds.com/news-and-insights/risk-reports/library/safeguarding-reputation</a>
2020	Lloyd's	Data Puts Active Portfolio Management on a Firm Footing	Case Study	<a href="https://www.lloyds.com/news-and-insights/risk-reports/library/data-puts-active-portfolio-management-on-a-firm-footing">https://www.lloyds.com/news-and-insights/risk-reports/library/data-puts-active-portfolio-management-on-a-firm-footing</a>
2020	Lloyd's	Cities at Risk – Building a Resilient Future for the World's Urban Centres	Case Study	<a href="https://www.lloyds.com/news-and-insights/risk-reports/library/cities-at-risk">https://www.lloyds.com/news-and-insights/risk-reports/library/cities-at-risk</a>
2020	Lloyd's	Building Simpler Insurance Products to Better Protect Customers	Case Study	<a href="https://www.lloyds.com/news-and-insights/market-communications/covid-19/lloyds-covid19-response-package/building-simpler-insurance-products-to-better-protect-customers">https://www.lloyds.com/news-and-insights/market-communications/covid-19/lloyds-covid19-response-package/building-simpler-insurance-products-to-better-protect-customers</a>
2020	Lloyd's	Protecting Intangible Assets: Preparing for a New Reality	Case Study	<a href="https://www.lloyds.com/news-and-insights/risk-reports/library/lloyds-intangibles">https://www.lloyds.com/news-and-insights/risk-reports/library/lloyds-intangibles</a>
2019	Lloyd's	Shen Attack - Cyber Risk In Asia Pacific Ports	Case Study	<a href="https://www.lloyds.com/news-and-insights/risk-reports/library/shen-attack-cyber-risk-in-asia-pacific-ports">https://www.lloyds.com/news-and-insights/risk-reports/library/shen-attack-cyber-risk-in-asia-pacific-ports</a>
2019	Lloyd's	Bashe Attack - Global Infection by Contagious Malware	Case Study	<a href="https://www.lloyds.com/news-and-insights/risk-reports/library/bashe-attack">https://www.lloyds.com/news-and-insights/risk-reports/library/bashe-attack</a>
2018	Lloyd's	Networked World - Risks and Opportunities in the Internet of Things	Case Study	<a href="https://www.lloyds.com/news-and-insights/risk-reports/library/networked-world">https://www.lloyds.com/news-and-insights/risk-reports/library/networked-world</a>
2019	Lloyd's	Taking Control - Artificial Intelligence and Insurance	Case Study	<a href="https://www.lloyds.com/news-and-insights/risk-reports/library/taking-control">https://www.lloyds.com/news-and-insights/risk-reports/library/taking-control</a>
2018	Lloyd's	New Realities - Risks in the Virtual World	Case Study	<a href="https://www.lloyds.com/news-and-insights/risk-reports/library/new-realities">https://www.lloyds.com/news-and-insights/risk-reports/library/new-realities</a>
2017	Lloyd's	Counting the Cost - Cyber Exposure Decoded	Case Study	<a href="https://www.lloyds.com/news-and-insights/risk-reports/library/countingthecost">https://www.lloyds.com/news-and-insights/risk-reports/library/countingthecost</a>
2010	Lloyd's	Managing Digital Risk - Trends, Issues and Implications for Business	Case Study	<a href="https://www.lloyds.com/news-and-insights/risk-reports/library/technology/managing-digital-risk">https://www.lloyds.com/news-and-insights/risk-reports/library/technology/managing-digital-risk</a>
2017	Lloyd's	Stochastic Modelling of Liability Accumulation Risk	Case Study	<a href="https://assets.lloyds.com/assets/pdf-arium-stochastic-modelling/1/pdf-arium-stochastic-modelling.pdf">https://assets.lloyds.com/assets/pdf-arium-stochastic-modelling/1/pdf-arium-stochastic-modelling.pdf</a>
2021	MacColl, Nurse and Sullivan	Cyber Insurance and the Cyber Security Challenge	Challenges	<a href="https://static.rusi.org/247-op-cyber-insurance-v2.pdf">https://static.rusi.org/247-op-cyber-insurance-v2.pdf</a>

Year	Author/Organization	Title	Category	URL
2020	Marciano	How Much Does Cyber Insurance Cost? Cyber Insurance   Data Breach Insurance Premiums	Pricing	<a href="https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums/">https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums/</a>
2020	Marsh	Writing Clear Contracts for Cyber Risk Transfer	Clear contracts	<a href="https://www.marsh.com/uk/services/cyber-risk/insights/writing-contracts-cyber-risk-transfer.html">https://www.marsh.com/uk/services/cyber-risk/insights/writing-contracts-cyber-risk-transfer.html</a>
2020	Marsh	Silent Cyber: Managing Cyber Coverage within a Changing Insurance Market	Market	<a href="https://www.marsh.com/uk/services/cyber-risk/insights/silent-cyber-managing-coverage-in-changing-insurance-market.html">https://www.marsh.com/uk/services/cyber-risk/insights/silent-cyber-managing-coverage-in-changing-insurance-market.html</a>
2020	Marsh	Global Insurance Pricing Continues to Increase in First Quarter 2020	Market	<a href="https://www.marsh.com/uk/services/international-placement-services/insights/global-insurance-pricing-continues-to-increase-in-first-quarter-2020.html">https://www.marsh.com/uk/services/international-placement-services/insights/global-insurance-pricing-continues-to-increase-in-first-quarter-2020.html</a>
2022	Marsh	Global Insurance Market Index - 2022 Q1	Market	<a href="https://info.marsh.com/l/395202/2022-04-26/c769hd/395202/16509910878h7JyNnA/GIMI_Q1_2022_report.pdf">https://info.marsh.com/l/395202/2022-04-26/c769hd/395202/16509910878h7JyNnA/GIMI_Q1_2022_report.pdf</a>
2020	Marsh McLennan	MMC Cyber Handbook 2021	Market	<a href="https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2020/october/MMC_Cyber_Handbook_2021.pdf">https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2020/october/MMC_Cyber_Handbook_2021.pdf</a>
2021	NAIC	Report on the Cybersecurity Insurance Market	Market	<a href="https://content.naic.org/sites/default/files/index-cmte-c-Cyber_Supplement_2020_Report.pdf">https://content.naic.org/sites/default/files/index-cmte-c-Cyber_Supplement_2020_Report.pdf</a>
2020	National Institute of Standards and Technology	NIST PRIVACY FRAMEWORK		<a href="https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf">https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf</a>
2021	NetDiligence	Cyber Claims Study	Market	<a href="https://library.cyentia.com/report/report_008228.html">https://library.cyentia.com/report/report_008228.html</a>
2020	O'Brien et al.	Looking Beyond the Clouds: A U.S. Cyber Insurance Industry Catastrophe Loss Study	Catastrophic cyber risks	<a href="https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2020/october/Beyond-the-Clouds.pdf">https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2020/october/Beyond-the-Clouds.pdf</a>
2020	OECD	Encouraging Clarity in Cyber Insurance Coverage	Silent Cyber	<a href="https://www.oecd.org/daf/fin/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf">https://www.oecd.org/daf/fin/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf</a>
2020	OECD	Enhancing the Availability of Data for Cyber Insurance Underwriting	Data availability	<a href="https://www.oecd.org/daf/fin/insurance/Enhancing-the-Availability-of-Data-for-Cyber-Insurance-Underwriting.pdf">https://www.oecd.org/daf/fin/insurance/Enhancing-the-Availability-of-Data-for-Cyber-Insurance-Underwriting.pdf</a>
2017	OECD	The Cyber Insurance Market: Responding to a Risk with Few Boundaries	Market	<a href="https://www.oecd-ilibrary.org/finance-and-investment/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en">https://www.oecd-ilibrary.org/finance-and-investment/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en</a>
2017	OECD	Enhancing the Role of Insurance in Cyber Risk Management	Insurance as incentive	<a href="https://www.oecd-ilibrary.org/finance-and-investment/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en">https://www.oecd-ilibrary.org/finance-and-investment/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en</a>
2017	OECD	Supporting an Effective Cyber Insurance Market - OECD Report for the G7 Presidency	Market	<a href="https://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf">https://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf</a>

Year	Author/Organization	Title	Category	URL
2018	OECD	Unleashing the Potential of the Cyber Insurance Market - Conference Outcomes	Market	<a href="https://www.oecd.org/daf/fin/insurance/Unleashing-Potential-Cyber-Insurance-Market-Summary.pdf">https://www.oecd.org/daf/fin/insurance/Unleashing-Potential-Cyber-Insurance-Market-Summary.pdf</a>
2020	OECD	Insurance Coverage for Cyber Terrorism in Australia	Catastrophic cyber risks	<a href="https://www.oecd.org/finance/insurance/Insurance-Coverage-for-Cyber-Terrorism-in-Australia.htm">https://www.oecd.org/finance/insurance/Insurance-Coverage-for-Cyber-Terrorism-in-Australia.htm</a>
2020	QOMPLX	Mind the Gap	Systemic risks	<a href="https://library.cyentia.com/report/report_003468.html">https://library.cyentia.com/report/report_003468.html</a>
2020	Reagan et al.	Cyber Insurance Purchasing Grows Again in 2019	Market	<a href="https://www.marshmcclennan.com/content/dam/marsh/Documents/PDF/US-en/cyber-insurance-purchasing-report.pdf">https://www.marshmcclennan.com/content/dam/marsh/Documents/PDF/US-en/cyber-insurance-purchasing-report.pdf</a>
2016	Risk Management Solutions, Inc.	Managing Cyber Insurance Accumulation Risk	Framework	<a href="https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-rms-managing-cyber-insurance-accumulation-risk.pdf">https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-rms-managing-cyber-insurance-accumulation-risk.pdf</a>
2014	Ruffle et al.	Stress Test Scenario: Sybil Logic Bomb Cyber Catastrophe	Case Study	<a href="https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-sybil-logic-bomb-cyber-catastrophe-stress-test.pdf">https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-sybil-logic-bomb-cyber-catastrophe-stress-test.pdf</a>
2020	Sullivan and Nurse	Cyber Security Incentives and the Role of Cyber Insurance	Insurance as incentive	<a href="https://static.rusi.org/246_ei_cyber_insurance_final_web_version.pdf">https://static.rusi.org/246_ei_cyber_insurance_final_web_version.pdf</a>
2020	Tatar et al.	Quantification of Cyber Risk for Actuaries An Economic-Functional Approach	Model	<a href="https://www.soa.org/49c222/globalassets/assets/files/resources/research-report/2020/quantification-cyber-risk.pdf">https://www.soa.org/49c222/globalassets/assets/files/resources/research-report/2020/quantification-cyber-risk.pdf</a>
2019	Tracy	Could NIST SP 800-171 Be A Model for the Cyber Insurance Industry?	Framework	<a href="https://www.telos.com/blog/2019/07/10/nist-800-171b-cyber-insurance/">https://www.telos.com/blog/2019/07/10/nist-800-171b-cyber-insurance/</a>
2021	U. S. Government Accountability Office	Cyber Insurance	Challenges	<a href="https://www.gao.gov/products/gao-21-477">https://www.gao.gov/products/gao-21-477</a>
2022	U. S. Government Accountability Office	Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks	Challenges	<a href="https://www.gao.gov/assets/gao-22-104256.pdf">https://www.gao.gov/assets/gao-22-104256.pdf</a>
2020	U.S. Cyberspace Solarium Commission	The Cyberspace Solarium Commission Report: A Warning from Tomorrow	Challenges	<a href="https://drive.google.com/file/d/1ryMCIL_dZ30QyiFqFkkf10MxIXGT4yv/view">https://drive.google.com/file/d/1ryMCIL_dZ30QyiFqFkkf10MxIXGT4yv/view</a>
2020	Willis Tower Watson	Cyber Claims Analysis Report	Market	<a href="https://www.willistowerswatson.com/-/media/WTW/Insights/2020/07/cyber-claims-analysis-report.pdf">https://www.willistowerswatson.com/-/media/WTW/Insights/2020/07/cyber-claims-analysis-report.pdf</a>
2020	Wolfram	Building a Sustainable Cyber Insurance Market	Market	<a href="https://www.oecd.org/daf/fin/insurance/Building-a-Sustainable-Cyber-Insurance-Market.pdf">https://www.oecd.org/daf/fin/insurance/Building-a-Sustainable-Cyber-Insurance-Market.pdf</a>
2022	World Economic Forum	The Global Risks Report 2022	Market	<a href="https://www.marshmcclennan.com/content/dam/mmc-web/insights/publications/2022/global-risks-report-2022/global-risks-report-2022.pdf">https://www.marshmcclennan.com/content/dam/mmc-web/insights/publications/2022/global-risks-report-2022/global-risks-report-2022.pdf</a>
2021	Zhang, Xu and Su	Modeling and Pricing Cybersecurity Risks in Fog Computing Based IoT Architectures	Model	<a href="https://www.soa.org/resources/research-reports/2021/cybersecurity-risks/">https://www.soa.org/resources/research-reports/2021/cybersecurity-risks/</a>

## APPENDIX C: COMPENDIUM OF ACADEMIC LITERATURE

Year	Author	Publication Title	Risk Analysis Technique	Modeling Focus	Modeling Methodology	Scalability	Generability	Cyber Incident	URL
2021	Acharya et al.	Cyber Insurance Against Cyberattacks on Electric Vehicle Charging Stations	Case Study	severity	Game-theoretic model, optimization	Medium	Low	Business Interruption	<a href="https://doi.org/10.1109/TSG.2021.3133536">https://doi.org/10.1109/TSG.2021.3133536</a>
2018	Aditya et al.	RiskWriter: Predicting Cyber Risk of an Enterprise	Analysis of Business Documentation	severity and frequency	Game-theoretic model, optimization	Medium	Medium	General	<a href="https://doi.org/10.1007/978-3-030-05171-6_5">https://doi.org/10.1007/978-3-030-05171-6_5</a>
2021	Antonio et al.	Cyber Insurance Ratemaking: A Graph Mining Approach	Simulation	frequency	Graph mining	Medium	High	General	<a href="https://doi.org/10.3390/risks9120224">https://doi.org/10.3390/risks9120224</a>
2021	Antonio et al.	Pricing of cyber insurance premiums using a Markov-based dynamic model with clustering structure	Simulation	risk	Markov-based dynamic model, epidemic inhibition function (spread models), clustering	Medium	High	General	<a href="https://doi.org/10.1371/journal.pone.0258867">https://doi.org/10.1371/journal.pone.0258867</a>
2021	Awiszus et al.	Modeling and Pricing Cyber Insurance – A Survey	Statistical Analysis	frequency, severity	collective risk model, frequency-severity approach; dependence modeling; epidemic spread models, game theoretic models	High	High	General	
2019	Bandyopadhyay & Mookerjee	A model to analyze the challenge of using cyber insurance	Scenario Analysis	severity	Backward analysis of myriad breach scenarios	Medium	Medium	Data Breach	<a href="https://doi.org/10.1371/journal.pone.0258867">https://doi.org/10.1371/journal.pone.0258867</a>
2018	Barreto et al.	Cyber-Insurance for Cyber-Physical Systems	Case Study	severity	Generalized extreme value distribution	Medium	Medium	Extreme Events	<a href="https://doi.org/10.1109/CCTA.2018.8511535">https://doi.org/10.1109/CCTA.2018.8511535</a>
2021	Bessy-Roland et al.	Multivariate Hawkes process for cyber insurance	Breach Data Analysis	frequency, severity	Multi-variate Hawkes model	High	High	Data Breach	<a href="https://doi.org/10.1017/S1748499520000093">https://doi.org/10.1017/S1748499520000093</a>
2018	Bodin et al.	Cybersecurity insurance and risk-sharing	Scenario Analysis	risk	RISK ladder valuation	Medium	Low	Data Breach	<a href="https://doi.org/10.1016/j.jaccpubpol.2018.10.004">https://doi.org/10.1016/j.jaccpubpol.2018.10.004</a>
2006	Böhme & Kataria	On the Limits of Cyber-Insurance	Simulation	risk	t-copula to model cross-firm risks	Medium	Medium	General	<a href="https://doi.org/10.1007/118246334">https://doi.org/10.1007/118246334</a>
2019	Bohme et al.	A Fundamental Approach to Cyber Risk Analysis	Review	risk	economic modeling, actuarial modeling	High	High	General	<a href="https://informationsecurity.uibk.ac.at/pdfs/BLR2019_Fu">https://informationsecurity.uibk.ac.at/pdfs/BLR2019_Fu</a>

Year	Author	Publication Title	Risk Analysis Technique	Modeling Focus	Modeling Methodology	Scalability	Generability	Cyber Incident	URL
									<a href="#">ndamental Approach Cyber Risk Insurance Variance.pdf</a>
2022	Carriante et al.	Vine Copula Modelling Dependence Among Cyber Risks: A Dangerous Regulatory Paradox	Statistical Analysis	risk	vine copula	Medium	High	General	<a href="https://doi.org/10.2139/ssrn.4041750">https://doi.org/10.2139/ssrn.4041750</a>
2019	Carfora & Orlando	Quantile based risk measures in cyber security	Simulation	frequency, severity	linear regression model	High	High	Data Breach	<a href="https://doi.org/10.1109/CyberSA.2019.8899431">https://doi.org/10.1109/CyberSA.2019.8899431</a>
2022	Carfora & Orlando	Cyber Risk: Estimates for Malicious and Negligent Breaches Distributions	Case Study	frequency, severity	negative binomial distribution, skew-normal distribution, value at risk	Medium	Medium	Data Breaches	<a href="https://doi.org/10.1007/978-3-030-99638-3_23">https://doi.org/10.1007/978-3-030-99638-3_23</a>
2019	Carfora et al.	Cyber risk management: an actuarial point of view	Scenario Analysis	frequency, severity	binomial, lognormal, and skew-normal models	High	High	Data Breach	<a href="https://doi.org/10.2134/JOP.2019.231">https://doi.org/10.2134/JOP.2019.231</a>
2019	Egan et al.	Cyber operational risk scenarios for insurance companies	Scenario Analysis	frequency, severity	detailed scenarios	High	High	Internal Data Breach, Extortion, Hack	<a href="https://doi.org/10.1017/S1357321718000284">https://doi.org/10.1017/S1357321718000284</a>
2018	Eling & Jung	Copula approaches for modeling cross-sectional dependence of data breach losses	Breach Data Analysis	frequency, severity	non-zero Pair copula dependence modeling	Medium	Medium	Data Breach	<a href="https://doi.org/10.1016/j.insmatheco.2018.07.003">https://doi.org/10.1016/j.insmatheco.2018.07.003</a>
2022	Eling & Jung	Heterogeneity in cyber loss severity and its impact on cyber risk measurement	Cyber Loss Data Analysis	frequency, severity	Tweedie model	Medium	Medium	General	<a href="https://doi.org/10.1057/s41283-022-00095-w">https://doi.org/10.1057/s41283-022-00095-w</a>
2017	Eling & Loperfido	Data breaches: Goodness of fit, pricing, and risk measurement	Breach Data Analysis	frequency, severity	Multidimensional scaling, multiple factor analysis, and goodness of fit tests	Medium	Medium	Data Breach	<a href="https://doi.org/10.1016/j.insmatheco.2017.05.008">https://doi.org/10.1016/j.insmatheco.2017.05.008</a>
2019	Eling & Wirfs	What are the actual costs of cyber risk events?	Breach Data Analysis	frequency, severity	Loss distribution approach. Peaks-over-threshold method from extreme value theory. GLM for Poisson and negative binomial distribution (frequency). EVT with POT and dynamic extension for severity.	Medium	Medium	Data Breach, Business Interrupted	<a href="https://doi.org/10.1016/j.eior.2018.07.021">https://doi.org/10.1016/j.eior.2018.07.021</a>

Year	Author	Publication Title	Risk Analysis Technique	Modeling Focus	Modeling Methodology	Scalability	Generability	Cyber Incident	URL
2022	Eling et al.	Unraveling heterogeneity in cyber risks using quantile regressions	Statistical Analysis	frequency, severity	quantile regression	Medium	High	Data Breaches	<a href="https://doi.org/10.1016/j.insmatheco.2022.03.001">https://doi.org/10.1016/j.insmatheco.2022.03.001</a>
2022	Eling et al.	The Economic Impact of Extreme Cyber Risk Scenarios	Scenario Analysis	frequency, severity	economic impact analysis of six well-known scenarios	High	High	Extreme cyber incidents	<a href="https://doi.org/10.1080/10920277.2022.2034507">https://doi.org/10.1080/10920277.2022.2034507</a>
2017	Erdogan et al.	A Method for Developing Algorithms for Assessing Cyber-Risk Cost	Scenario Analysis	frequency	CORAS, a model-driven risk analysis; Calculations for this model are conducted in R via Monte Carlo	Medium	Medium	General	<a href="https://doi.org/10.1109/QRS.2017.729">https://doi.org/10.1109/QRS.2017.729</a>
2022	Erola et al.	A system to calculate Cyber Value-at-Risk	Case Study	risk	Probabilistic density function. Value at Risk models and Monte Carlo simulations to arrive at CVaR; normal and lognormal distributions, harm tree scenarios	Medium	Medium	General	<a href="https://doi.org/10.1016/j.cose.2021.102545">https://doi.org/10.1016/j.cose.2021.102545</a>
2018	Fahrenwaldt et al.	Pricing of Cyber Insurance Contracts in a Network Model	Simulation	frequency, severity	polynomial approx., mean-field approx.; exact loss model; "cyber infection spreads in a network, modeled by an interacting Markov process. Second, infected, i.e., vulnerable agents incur losses due to cyber attacks that occur according to a point process."	Medium	Low	General	<a href="https://doi.org/10.1017/asb.2018.23">https://doi.org/10.1017/asb.2018.23</a>
2021	Farkas et al.	Cyber claim analysis using Generalized Pareto regression trees with applications to insurance	Breach Data Analysis	extreme events	generalized Pareto modeling, extreme value theory, regression tree approach	Medium	Medium	Data Breach	<a href="https://doi.org/10.1016/j.insmatheco.2021.02.009">https://doi.org/10.1016/j.insmatheco.2021.02.009</a>
2021	Feng et al.	On Cyber Risk Management of Blockchain Networks: A Game Theoretic Approach	Game Theory Analysis	risk	assumption of rationality for the market entities, game-theoretic model (two-level Stackelberg game)	Low	Low	Business Interruption	<a href="https://doi.org/10.1109/TSC.2018.2876846">https://doi.org/10.1109/TSC.2018.2876846</a>
2018	Feng et al.	Competitive Security Pricing in Cyber-Insurance Market: A Game-Theoretic Analysis	Game Theory Analysis	risk	Game-theoretic model (Stackelberg game)	Medium	Medium	General	<a href="https://doi.org/10.1109/VTCFall.2018.8690762">https://doi.org/10.1109/VTCFall.2018.8690762</a>
2021	Feng et al.	Dynamic Resource Management to Defend Against	Game Theory Analysis	frequency	Game-theoretic model (Stackelberg game)	Medium	Low	Data Breach (APT)	<a href="https://doi.org/10.1109/">https://doi.org/10.1109/</a>

Year	Author	Publication Title	Risk Analysis Technique	Modeling Focus	Modeling Methodology	Scalability	Generability	Cyber Incident	URL
		Advanced Persistent Threats in Fog Computing: A Game Theoretic Approach							<a href="https://doi.org/10.2896632">9/TCC.2019.2896632</a>
2019	Franke & Draeger	Two simple models of business interruption accumulation risk in cyber insurance	Model Analysis	frequency	Poisson distribution, log-normal distribution	Medium	Medium	Business Interruption	<a href="https://doi.org/10.1109/CyberSA.2019.8899678">https://doi.org/10.1109/CyberSA.2019.8899678</a>
2022	Gatzert & Schubert	Cyber risk management in the U.S. banking and insurance industry: A textual and empirical analysis of determinants and value	Statistical Analysis	risk	rules-based text mining, logistic regression	Medium	Medium	General	<a href="https://doi.org/10.1111/jori.12381">https://doi.org/10.1111/jori.12381</a>
2015	Hayel & Zhu	Attack-Aware Cyber Insurance for Risk Sharing in Computer Networks	Game Theory Analysis	risk	Game-theoretic model; games-in-games framework (Nash Equilibria, sequential game)	Medium	Medium	General	<a href="https://doi.org/10.1007/978-3-319-25594-1_2">https://doi.org/10.1007/978-3-319-25594-1_2</a>
2021	Hillairet & Lopez	Propagation of cyber incidents in an insurance portfolio: counting processes combined with compartmental epidemiological models	Simulation	frequency	compartmental epidemiological models, Gaussian approximations	High	High	General	<a href="https://doi.org/10.1080/03461238.2021.1872694">https://doi.org/10.1080/03461238.2021.1872694</a>
2021	Hua & Xu	Pricing Cyber Insurance for a Large-Scale Network	Simulation	frequency	Scale-free network, static scale-free random graph, simulation, linear and generalized linear models based on gamma distribution and inverse Gaussian distribution?	Medium	Medium	General	
2018	Insua et al.	Some Risk Analysis Problems in Cyber Insurance Economics	Model Analysis	frequency	influence diagrams and bi-agent influence diagrams of three models	Medium	Medium	General	
2021	Insua et al.	An Adversarial Risk Analysis Framework for Cybersecurity	Case Study	frequency, severity	influence diagrams and bi-agent influence diagrams of cybersecurity adversarial risk analysis approach; illustrated with a defense-attack case study	Medium	Medium	General	<a href="https://doi.org/10.1111/risa.13331">https://doi.org/10.1111/risa.13331</a>
2020	Jevtić & Lanchier	Dynamic structural percolation model of loss distribution for cyber risk of small and medium-sized	Model Analysis	risk	random tree graphs (LAN topology), cost topology, percolation model, probabilistic	Medium	Medium	Data Breach	<a href="https://doi.org/10.1016/j.insmath.2020.02.005">https://doi.org/10.1016/j.insmath.2020.02.005</a>

Year	Author	Publication Title	Risk Analysis Technique	Modeling Focus	Modeling Methodology	Scalability	Generability	Cyber Incident	URL
		enterprises for tree-based LAN topology			graph-theoretical framework				
2014	Johnson et al.	How Many down? Toward Understanding Systematic Risk in Networks	Simulation	risk	the risk propagation model is borrowed from the literature on interdependent security games, where it has been used primarily to study the incentives of individuals within a networked system; simulation algorithm to approx. loss distribution	Medium	Medium	General	<a href="https://doi.org/10.1145/2590296.2590308">https://doi.org/10.1145/2590296.2590308</a>
2021	Jung	Extreme Data Breach Losses: An Alternative Approach to Estimating Probable Maximum Loss for Data Breach Risk	Breach Data Analysis	frequency, severity	generalized extreme value distribution, time-series, and extreme value analysis	Medium	High	Data Breach	<a href="https://doi.org/10.1080/1092027.2021.1919145">https://doi.org/10.1080/1092027.2021.1919145</a>
2017	Kelliher et al.	Good practice guide to setting inputs for operational risk models	Scenario Analysis	risk	scenario analysis	High	High	Data loss	<a href="https://doi.org/10.1017/S1357321716000179">https://doi.org/10.1017/S1357321716000179</a>
2018	Khalili et al.	Designing Cyber Insurance Policies: The Role of Pre-Screening and Security Interdependence	Model Analysis	risk	game-theoretic model	Medium	Medium	General	<a href="https://doi.org/10.1109/TIFS.2018.2812205">https://doi.org/10.1109/TIFS.2018.2812205</a>
2017	Khalili et al.	Embracing Risk Dependency in Designing Cyber-Insurance Contracts	Scenario Analysis	risk	interdependent network model; simple two-agent, two-insurer model	Medium	Medium	General	<a href="https://doi.org/10.1109/ALLERTON.2017.8262837">https://doi.org/10.1109/ALLERTON.2017.8262837</a>
2019	Khalili et al.	Embracing and controlling risk dependency in cyber-insurance policy underwriting	Scenario Analysis	risk	standard underwriting framework (base rate insurance policy framework) to look at different portfolio choices and quantify impact; model three different portfolio alternatives	Medium	Medium	Data Breach, Business Interrupted	<a href="https://doi.org/10.1093/cybsec/tyz010">https://doi.org/10.1093/cybsec/tyz010</a>
2019	Khalili et al.	Effective Premium Discrimination for Designing Cyber Insurance Policies with Rare Losses	Scenario Analysis	frequency, severity	contract theory framework based on the attack model	Medium	Medium	Data Breach, Loss events	<a href="https://doi.org/10.1007/978-3-030-32430-8_16">https://doi.org/10.1007/978-3-030-32430-8_16</a>
2018	Laszka et al.	On the Assessment of Systematic Risk in Networked Systems	Simulation	risk	a multiple-hop variant of propagation model; proof for NP-hardness, loss-number	Medium	Medium	General	<a href="https://doi.org/10.1145/3166069">https://doi.org/10.1145/3166069</a>



Year	Author	Publication Title	Risk Analysis Technique	Modeling Focus	Modeling Methodology	Scalability	Generability	Cyber Incident	URL
					distribution, builds on interdependent security game, game-theoretic model				
2014	Laszka et al.	Estimating Systematic Risk in Real-World Networks	Simulation	risk	network risk model/ risk propagation model builds on a framework for interdependent security games; loss distributions	Medium	High	General	<a href="https://doi.org/10.1007/978-3-662-45472-5_27">https://doi.org/10.1007/978-3-662-45472-5_27</a>
2022	Lau et al.	A Novel Mutual Insurance Model for Hedging Against Cyber Risks in Power Systems Deploying Smart Technologies	Simulation	risk	stochastic Epidemic Network Model, optimization	Medium	Medium	General	<a href="https://doi.org/10.1109/TPWRS.2022.3164628">https://doi.org/10.1109/TPWRS.2022.3164628</a>
2021	Lau et al.	A Coalitional Cyber-Insurance Design Considering Power System Reliability and Cyber Vulnerability	Simulation	risk	cyber model of network vulnerability via attack graph/ tree, game theoretic algorithms	Medium	Low	General	<a href="https://doi.org/10.1109/TPWRS.2021.3078730">https://doi.org/10.1109/TPWRS.2021.3078730</a>
2020	Li et al.	A Contract-Theoretic Cyber Insurance for Withdraw Delay in the Blockchain Networks with Shards	Simulation	risk	contract theoretic framework and system model (discouragement attack model, the reward distribution function, the expected loss, utility models for validation)	Low	Low	General	<a href="https://doi.org/10.1109/ICC4027.7.2020.9149437">https://doi.org/10.1109/ICC4027.7.2020.9149437</a>
2021	Lin et al.	Pricing Cyber Security Insurance	Event Study	frequency, severity	total loss model, aggregate loss model	High	Medium	Data breaches	<a href="https://doi.org/10.4236/jmf.2022.121003">https://doi.org/10.4236/jmf.2022.121003</a>
2021	Liu	Embracing Risk: Cyber Insurance as an Incentive Mechanism for Cybersecurity	Game Theory Analysis	frequency, severity	basic cyber insurance contract model (single agent - single period model, single agent-multi period model); model of two agents; insurance policy model	High	High	General	<a href="https://doi.org/10.2200/S01093ED1V01Y202104LNAO26">https://doi.org/10.2200/S01093ED1V01Y202104LNAO26</a>
2022	Liu et al.	Bayesian vine copulas for modelling dependence in data breach losses	Simulation	severity	vine copulas under Bayesian framework, vine copula and pairwise copulas modelling	Medium	Medium	Data Breach	<a href="https://doi.org/10.1017/S174849952200001X">https://doi.org/10.1017/S174849952200001X</a>
2021	Liu et al.	An Extreme Value Theory Based Catastrophe Bond Design for Cyber Risk Management of Power Systems	Simulation	frequency, severity	extreme value theory, stochastic model	Medium	Low	General (malicious cyberattacks)	<a href="https://doi.org/10.1109/TSG.2021.3131468">https://doi.org/10.1109/TSG.2021.3131468</a>
2021	Liu et al.	An Actuarial Framework for Power System Reliability	Simulation	risk	actuarial theory, semi-Markov process, Monte Carlo simulations framework, temporal	Medium	Low	General	<a href="https://doi.org/10.1109/TPWRS.2021.3078730">https://doi.org/10.1109/TPWRS.2021.3078730</a>

Year	Author	Publication Title	Risk Analysis Technique	Modeling Focus	Modeling Methodology	Scalability	Generability	Cyber Incident	URL
		Considering Cybersecurity Threats			diversification technique				<a href="https://doi.org/10.1109/TCOM.2018.1700501">020.3018701</a>
2018	Lu et al.	Cyber Insurance for Heterogeneous Wireless Networks	Simulation	risk	Poisson process, Monte Carlo simulations	Medium	Low	General	<a href="https://doi.org/10.1109/MCOM.2018.1700504">https://doi.org/10.1109/MCOM.2018.1700504</a>
2018	Meland & Seehusen	When to Treat Security Risks with Cyber Insurance	Simulation	frequency	generic risk model	High	High	General	<a href="https://doi.org/10.1109/CyberSA.2018.8551456">https://doi.org/10.1109/CyberSA.2018.8551456</a>
2019	Mukhopadhyay et al.	Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance	Statistical Analysis	frequency, severity	collective risk modelling; generalized linear models (GLM), namely logit and probit; gamma and exponential distribution	Medium	Medium	General	<a href="https://doi.org/10.1007/s10796-017-9808-5">https://doi.org/10.1007/s10796-017-9808-5</a>
2010	Pal & Golubchik	On the Economics of Information Security: The Problem of Designing Optimal Cyber-Insurance Contracts	Scenario Analysis	risk	game theoretic models, optimization	Medium	Medium	General	<a href="https://doi.org/10.1145/1870178.1870196">https://doi.org/10.1145/1870178.1870196</a>
2012	Pal & Hui	Cyber Insurance for Cybersecurity a Topological Take on Modulating Insurance Premiums	Game Theory Analysis	risk	game-theoretic model; Von Neumann Morgenstern utility function; justify using Bonacich or eigenvector centrality	Medium	Medium	General	<a href="https://doi.org/10.1145/2425248.2425271">https://doi.org/10.1145/2425248.2425271</a>
2019	Pal et al.	On Robust Estimates of Correlated Risk in Cyber-Insured IT Firms: A First Look at Optimal AI-Based Estimates under "Small" Data	Simulation	risk	Optimization, conditional density function using copula, cyber-vulnerability assessment (C-VA) model from Mukhopadhyay et al. (2013) for both MCOP and the CBBN methodology.	Medium	Low	General	<a href="https://doi.org/10.1145/3351158">https://doi.org/10.1145/3351158</a>
2019	Pal et al.	Security Pricing as Enabler of Cyber-Insurance A First Look at Differentiated Pricing Markets	Simulation	risk	Stackelberg games, Nash equilibrium, spectral graph theory, topologies (scale-free graphs and trees)	Medium	Medium	General	<a href="https://doi.org/10.1109/TDSC.2017.2684801">https://doi.org/10.1109/TDSC.2017.2684801</a>
2021	Pal et al.	Aggregate Cyber-Risk Management in the IoT Age: Cautionary Statistics for (Re)Insurers and Likes	Simulation	frequency, severity	Monte Carlo simulations	Medium	Medium	Data Breach	<a href="https://doi.org/10.1109/IJOT.2020.3039254">https://doi.org/10.1109/IJOT.2020.3039254</a>
2020	Palsson et al.	Analysis of the impact of cyber	Cyber Loss Data Analysis	frequency, severity	Random Forests classifiers	Medium	Medium	Data Breach,	<a href="https://doi.org/10.105">https://doi.org/10.105</a>

Year	Author	Publication Title	Risk Analysis Technique	Modeling Focus	Modeling Methodology	Scalability	Generability	Cyber Incident	URL
		events for cyber insurance						Business Interrupted	<a href="https://doi.org/10.1109/TEM.2020.3028526">7/s41288-020-00171-w</a>
2021	Pate-Cornell & Kuyper s	A Probabilistic Analysis of Cyber Risks	Scenario Analysis	frequency , severity	general probabilistic risk analysis model (data-driven model and scenario-based model); monte Carlo simulation	Medium	Medium	General	<a href="https://doi.org/10.1109/TEM.2020.3028526">https://doi.org/10.1109/TEM.2020.3028526</a>
2017	Piromsopa et al.	Designing Model for Calculating the Amount of Cyber Risk Insurance	Use Case	risk	scoring model	Medium	Medium	General	<a href="https://doi.org/10.1109/MCSI.2017.41">https://doi.org/10.1109/MCSI.2017.41</a>
2018	Pooser et al.	Growth in the Perception of Cyber Risk: Evidence from U.S. P&C Insurers	Statistical Analysis	N/A	N/A	N/A	N/A	General	
2020	Poyraz et al.	Cyber assets at risk: monetary impact of U.S. personally identifiable information mega data breaches	Breach Data Analysis	frequency , severity	stepwise regression analysis (polynomial, factorial multilevel effects of IVs)	Medium	Medium	Data Breach that contains PII	<a href="https://doi.org/10.1057/s41288-020-00185-4">https://doi.org/10.1057/s41288-020-00185-4</a>
2019	Romanosky et al.	Content analysis of cyber insurance policies: how do carriers price cyber risk?	Thematic Analysis	N/A	N/A	N/A	N/A	Data breach and security incidents	<a href="https://doi.org/10.1093/cybsec/tyz002">https://doi.org/10.1093/cybsec/tyz002</a>
2011	Saini et al.	Utility Implementation for Cyber Risk Insurance Modeling	Scenario Analysis	risk	utility theory model	Medium	Low	Data breach	
2014	Schwarz & Sastry	Cyber-Insurance Framework for Large Scale Interdependent Networks	Game Theory Analysis	frequency	game-theoretic model	Low	High	Data breach	<a href="https://doi.org/10.1145/2566468.2566481">https://doi.org/10.1145/2566468.2566481</a>
2015	Shah et al.	Valuing Data Security and Privacy Using Cyber Insurance	Simulation	frequency , severity	classical loss distribution approach, Monte Carlo simulations	Medium	Medium	Data breach	<a href="https://doi.org/10.1145/2738210.2738217">https://doi.org/10.1145/2738210.2738217</a>
2022	Sharma & Mukhopadhyay	Sarima-Based Cyber-Risk Assessment and Mitigation Model for A Smart City's Traffic Management Systems (Scram)	Model Analysis	severity	SCRAM based on protection motivation theory; risk theory	Medium	Medium	General	<a href="https://doi.org/10.1080/10919392.2022.2054259">https://doi.org/10.1080/10919392.2022.2054259</a>
2022	Sharma & Mukhopadhyay	Cyber-risk Management Framework for Online Gaming Firms: An Artificial Neural Network Approach	Model Analysis	frequency , severity	three stages (cyber-risk assessment, cyber-risk quantification, and cyber-risk Mitigation); Feedforward Neural Network-based Cyber-risk Assessment and Mitigation model (FNN-CRAM) based on the opportunity theory of crime, rational	Medium	High	General	<a href="https://doi.org/10.1007/s10796-021-10232-7">https://doi.org/10.1007/s10796-021-10232-7</a>

Year	Author	Publication Title	Risk Analysis Technique	Modeling Focus	Modeling Methodology	Scalability	Generability	Cyber Incident	URL
					choice theory, and risk theory.				
2021	Sheehan et al.	A quantitative bow-tie cyber risk classification and assessment framework	Scenario Analysis	frequency, severity	bow-tie model with a risk matrix	Medium	Medium	General	<a href="https://doi.org/10.1080/13669877.2021.1900337">https://doi.org/10.1080/13669877.2021.1900337</a>
2010	Shetty et al.	Competitive Cyber-Insurance and Internet Security	Model Analysis	risk	utility theory model	Medium	Medium	General	<a href="https://doi.org/10.1007/978-1-4419-6967-5_12">https://doi.org/10.1007/978-1-4419-6967-5_12</a>
2018	Shetty et al.	Reducing Informational Disadvantages to Improve Cyber Risk Management†	Model Analysis	frequency, severity	Bayesian attack graph model	High	Medium	General	<a href="https://doi.org/10.1057/s41288-018-0078-3">https://doi.org/10.1057/s41288-018-0078-3</a>
2022	Skeoch	Expanding the Gordon-Loeb model to cyber-insurance	Simulation	risk	Gordon-Loeb model, exponential and logarithmic utility functions	Medium	Medium	General	<a href="https://doi.org/10.1016/j.cose.2021.102533">https://doi.org/10.1016/j.cose.2021.102533</a>
2019	Strupczewski	What Is the Worst Scenario? Modeling Extreme Cyber Losses	Statistical Analysis	risk	GPD statistical distribution/ analysis, heavy-tail distribution analysis	Medium	High	Extreme Cyber Risks	<a href="https://doi.org/10.1007/978-3-16045-610">https://doi.org/10.1007/978-3-16045-610</a>
2021	Sun et al.	Modeling Malicious Hacking Data Breach Risks	Breach Data Analysis	frequency, severity	hurdle Poisson model, non-parametric generalized Pareto distribution model	Medium	Medium	Data breach	<a href="https://doi.org/10.1080/10920277.2020.1752255">https://doi.org/10.1080/10920277.2020.1752255</a>
2019	Uuganbayar et al.	Cyber Insurance and Time-to-Compromise: An Integrated Approach	Statistical Analysis	frequency, severity	time-to-compromise metric applied to an algorithm	Medium	Medium	General	<a href="https://doi.org/10.1109/CyberSA.2019.8899442">https://doi.org/10.1109/CyberSA.2019.8899442</a>
2019	Vakilinia & Sengupta	A Coalitional Cyber-Insurance Framework for a Common Platform	Model Analysis	risk	system model; three models for insuring a common platform; ex-ante individual rationality	Medium	Medium	General	<a href="https://doi.org/10.1109/TIFS.2018.2881694">https://doi.org/10.1109/TIFS.2018.2881694</a>
2021	Verlaine	On the extraction of cyber risks from structured products	Theory Analysis	N/A	information theory, extreme risk modelling	Medium	High	General	<a href="https://doi.org/10.1080/00036846.2021.1998327">https://doi.org/10.1080/00036846.2021.1998327</a>
2019	Wang	Integrated framework for information security investment and cyber insurance	Model Analysis	severity	an analytical model based on reducing cyber threats, vulnerability, impact	Medium	Medium	Data Breach	<a href="https://doi.org/10.1016/j.pacfin.2019.101173">https://doi.org/10.1016/j.pacfin.2019.101173</a>
2020	Wang & Franke	Enterprise IT service downtime cost and risk transfer in a supply chain	Case Study	frequency	baseline probability model of Poisson arrival frequency with lognormal downtime	Medium	Medium	Business Interrupted	<a href="https://doi.org/10.1007/s12063-">https://doi.org/10.1007/s12063-</a>

Year	Author	Publication Title	Risk Analysis Technique	Modeling Focus	Modeling Methodology	Scalability	Generability	Cyber Incident	URL
					duration, propagation model				<a href="https://doi.org/10.1145/3409959">020-00148-x</a>
2021	Wang et al.	Game Theory Based Cyber-Insurance to Cover Potential Loss from Mobile Malware Exploitation	Simulation	risk	Algorithmic game theory, stochastic games	Low	Low	General	<a href="https://doi.org/10.1145/3409959">https://doi.org/10.1145/3409959</a>
2022	Watson et al.	The Impact of Purchasing Cyber Insurance on the Enhancement of Operational Cyber Risk Mitigation of U.S. Banks - A Case Study	Case Study	N/A	N/A	N/A	N/A	General	<a href="https://doi.org/10.1109/CCWC54503.2022.9720791">https://doi.org/10.1109/CCWC54503.2022.9720791</a>
2021	Welburn & Strong	Systemic Cyber Risk and Aggregate Impacts	Case Study	risk	input-output modelling	Medium	Medium	General	<a href="https://doi.org/10.1111/risa.13715">https://doi.org/10.1111/risa.13715</a>
2021	Woods et al.	The County Fair Cyber Loss Distribution: Drawing Inferences from Insurance Prices	Market Analysis	frequency	particle swarm optimization, polynomial distribution	Medium	Low	Business Interrupted, Fraud, PCI	<a href="https://doi.org/10.1145/3434403">https://doi.org/10.1145/3434403</a>
2020	Xie et al.	Cyber insurance offering and performance: an analysis of the U.S. cyber insurance market	Statistical Analysis	frequency, severity	logistic regression	Medium	Low	General	<a href="https://doi.org/10.1057/s41288-020-00176-5">https://doi.org/10.1057/s41288-020-00176-5</a>
2019	Xu & Hua	Cybersecurity Insurance: Modeling and Pricing	Simulation	frequency	epidemic models, loss functions, premium strategies; Markov and non-Markov models, copula; Monte Carlo simulations	Medium	Medium	General	<a href="https://doi.org/10.1080/10920277.2019.1566076">https://doi.org/10.1080/10920277.2019.1566076</a>
2021	Xu & Zhang	Data Breach CAT Bonds: Modeling and Pricing	Simulation	frequency	extreme value model, data-driven time series approaches	Medium	Medium	Data Breach	<a href="https://doi.org/10.1080/10920277.2021.1886948">https://doi.org/10.1080/10920277.2021.1886948</a>
2019	Yang et al.	Incentive Contract for Cybersecurity Information Sharing Considering Monitoring Signals	Model Analysis	risk	principal-agent theoretical model	Medium	Medium	General	<a href="https://doi.org/10.1109/iThings/GreenCom/CPSCoM/SmartData.2019.00103">https://doi.org/10.1109/iThings/GreenCom/CPSCoM/SmartData.2019.00103</a>
2019	Yang et al.	Optimal Model Design for the Cyber-Insurance Contract with Asymmetric Information	Model Analysis	risk	risk probability model; asymmetric and symmetric conditions using Pareto optimal risk sharing	Medium	Medium	General	<a href="https://doi.org/10.1109/iThings/GreenCom/CPSCoM/SmartData.2019.00104">https://doi.org/10.1109/iThings/GreenCom/CPSCoM/SmartData.2019.00104</a>

Year	Author	Publication Title	Risk Analysis Technique	Modeling Focus	Modeling Methodology	Scalability	Generability	Cyber Incident	URL
2020	Yang et al.	Premium Calculation for Insurance Businesses Based on Cyber Risks in IP-Based Power Substations	Simulation	frequency, severity	ruin theory, spatial correlation, test case	Medium	Medium	Business Interrupted	<a href="https://doi.org/10.1109/ACCESS.2020.2988548">https://doi.org/10.1109/ACCESS.2020.2988548</a>
2016	Young et al.	A framework for incorporating insurance in critical infrastructure cyber risk strategies	Scenario Analysis	frequency, severity	threat likelihood and severity model, Gordon-Loeb model, insurance premium discount model; optimization	High	Medium	General	<a href="https://doi.org/10.1016/j.ijcip.2016.04.001">https://doi.org/10.1016/j.ijcip.2016.04.001</a>
2021	Zeller & Scherer	A comprehensive model for cyber risk based on marked point processes and its application to insurance	Simulation	frequency, severity	loss distribution approach	Medium	Medium	General (breach, interruptions, fraud)	<a href="https://doi.org/10.1007/s13385-021-00290-1">https://doi.org/10.1007/s13385-021-00290-1</a>
2020	Zhang & Zhu	FlipIn: A Game-Theoretic Cyber Insurance Framework for Incentive-Compatible Cyber Risk Management of Internet of Things	Scenario Analysis	frequency	game-theoretic model, Peltzman effect	Medium	Low	APT	<a href="https://doi.org/10.1109/TIFS.2019.2955891">https://doi.org/10.1109/TIFS.2019.2955891</a>
2021	Zhang & Zhu	Optimal Cyber-Insurance Contract Design for Dynamic Risk Management and Mitigation	Experiment	risk	principal-agent model; Markov decision process; two-state two-action user under linear coverage insurance	Medium	Medium	General	<a href="https://doi.org/10.1109/TCSS.2021.3117905">https://doi.org/10.1109/TCSS.2021.3117905</a>
2017	Zhang et al.	A Bi-Level Game Approach to Attack-Aware Cyber Insurance of Computer Networks	Experiment	risk	game-theoretic model (zero-sum games in a moral-hazard type of principal-agent game), bi-level game	High	Medium	General	<a href="https://doi.org/10.1109/JSAC.2017.2672378">https://doi.org/10.1109/JSAC.2017.2672378</a>
2021	Zhang et al.	A Cyber-Insurance Scheme for Water Distribution Systems Considering Malicious Cyberattacks	Simulation	risk	semi-Markov process model, sequential monte Carlo simulation (MCS)	Medium	Low	General	<a href="https://doi.org/10.1109/TIFS.2020.3045902">https://doi.org/10.1109/TIFS.2020.3045902</a>

## APPENDIX D: COMPENDIUM OF CYBER INSURANCE DATASETS

Dataset	Available	Content	Years Covered	# of Records	Data Collection Method	Cyber Incident Type	Link	Relevant Articles
Advisen Cyber Loss Dataset	Available with fee	Count, Loss	2001-2022	90,000	Parsed publicly available data	Data/ system breaches and security violations	<a href="https://www.advisentd.com/data/cyber-loss-data/">https://www.advisentd.com/data/cyber-loss-data/</a>	Palsson et al.
Chronology of Data Breaches by Privacy Rights Clearinghouse (PRC)	Yes	Exposure, Count	2005-Present	8,804+	Parsed publicly available data collected by a U.S.-based non-profit organization	Data breaches	<a href="https://privacyrights.org/data-breaches">https://privacyrights.org/data-breaches</a>	<ul style="list-style-type: none"> <li>•Bessy-Roland et al.</li> <li>•Carfora &amp; Orlando</li> <li>•Carfora &amp; Orlando</li> <li>•Carfora et al.</li> <li>•Eling &amp; Jung</li> <li>•Eling &amp; Loperfido</li> <li>•Farkas et al.</li> <li>•Lin et al.</li> <li>•Sun et al.</li> <li>•Pal et al.</li> <li>•Liu et al.</li> <li>•Xu &amp; Zhang</li> <li>•Eling &amp; Wirfs</li> <li>•Poyraz et al.</li> </ul>
Internet Security Threat Report by Symantec	Yes	Exposure	Annual	-	Collection of data from global attack sensors	Cyber-attacks from around the world	<a href="https://www.broadcom.com/support/security-center">https://www.broadcom.com/support/security-center</a>	•Wang et al.
SAS OpRisk Global Dataset	Yes	Loss	1984-Present	37,652+	Parsed publicly available data on global cyber operational losses	Cyber operational losses	<a href="https://www.sas.com/content/dam/SAS/en_us/doc/productbrief/sas-oprisk-global-data-101187.pdf">https://www.sas.com/content/dam/SAS/en_us/doc/productbrief/sas-oprisk-global-data-101187.pdf</a>	<ul style="list-style-type: none"> <li>•Eling &amp; Wirfs</li> <li>•Eling &amp; Jung</li> <li>•Strupczewski</li> </ul>
Cyber AcuView	Available with fee	Loss, Exposure	N/A	-	Parse public industry data and privately collected industry information	Unintended data disclosure, Data breach, and others	<a href="https://cyberacuview.com/services/">https://cyberacuview.com/services/</a>	
DataLossDB by Risk Based Security	Yes	Exposure, Count	1995-Present	1,000+	Acquired from verifiable databases and government resources	Data breaches	<a href="http://datalossdb.org/primary-sources">http://datalossdb.org/primary-sources</a>	
DHS Impact	Yes	Exposure, Loss	2015-Present	-	Parsed publicly available data; entities provided cyber data	Publicly disclosed security incidents including data breaches	<a href="https://www.impactcybertrust.org/">https://www.impactcybertrust.org/</a>	
eRiskHub by NetDiligence	Available	Severity, Frequency,	2011-Present	-	Parsed from the insurance industry	Data from all cyber claims studies	<a href="https://eriskhub.com">https://eriskhub.com</a>	

Dataset	Available	Content	Years Covered	# of Records	Data Collection Method	Cyber Incident Type	Link	Relevant Articles
	with fee	and Data Exposure						
FBI Internet Crime Complaint Center (IC3)	Yes	Count, Loss	2000-Present	-	Parsed publicly available data	Internet-related crimes in the U.S. and around the world	<a href="https://www.ic3.gov/Home/AnnualReports">https://www.ic3.gov/Home/AnnualReports</a>	
ISO Verisk	Available with fee	Exposure, Loss	2010 - Present	100 million insights	Collected from participating insurers	N/A	<a href="https://www.verisk.com/insurance/products/cyber-insurance-program/">https://www.verisk.com/insurance/products/cyber-insurance-program/</a>	
ORX Operational Risk Data	Available with fee	Loss	2015-2020	-	Parsed publicly available data in the insurance and banking industry	Cyber operational risks	<a href="https://engage.orx.org/buy/annual-loss-reports">https://engage.orx.org/buy/annual-loss-reports</a>	
Cost of Data Breach Study by Ponemon Institute/ IBM Security	Yes	Count, Loss	Annual	Survey of 350 companies across 11 countries	Parsed publicly available data	Data breaches	<a href="https://www.capita.com/sites/g/files/nginei291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf">https://www.capita.com/sites/g/files/nginei291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf</a>	
VERIS Community Database (VCDB)	Yes	Count, Loss	2008-Present	8,500	Parsed publicly available data	Publicly disclosed security incidents including data breaches	<a href="http://veriscommunity.net/vcdb.html">http://veriscommunity.net/vcdb.html</a>	
Common Vulnerabilities and Exposures (CVE)	Yes	Vulnerability Classification	1990s-Present	177,307	Entry by security professionals and product vendors	N/A	<a href="https://cve.mitre.org/cve/cvrf.html">https://cve.mitre.org/cve/cvrf.html</a>	
Common Vulnerability Scoring System	Yes	Vulnerability Scoring	1990s-Present	177,270	Entry by security professionals and product vendors	N/A	<a href="https://nvd.nist.gov/vuln-metrics/cvss">https://nvd.nist.gov/vuln-metrics/cvss</a>	
Honeypot Projects by Honeynet	Yes	Malicious Attack Activity via Honeypots	N/A	-	Parsed from honeypot sensors placed globally	Malicious attacks	<a href="https://www.honeynet.org/projects/">https://www.honeynet.org/projects/</a>	



## References – Grey Literature

- Advisen & PartnerRe. (2020). *Cyber Insurance—The Market’s View* (p. 17). [https://library.cventia.com/report/report\\_005654.html](https://library.cventia.com/report/report_005654.html)
- Advisen & Zurich. (2020). *Information Security and Cyber Risk Management Report 2020* (p. 15). [https://library.cventia.com/report/report\\_006084.html](https://library.cventia.com/report/report_006084.html)
- Aite Novarica. (2016). *Cyber Insurance and Cybersecurity: The Convergence* (p. 81). [https://library.cventia.com/report/report\\_001099.html](https://library.cventia.com/report/report_001099.html)
- American Academy of Actuaries & Cyber Risk Task Force, Casualty Practice Council. (2022). *Cyber Risk Toolkit* (p. 89). American Academy of Actuaries. <https://www.actuary.org/sites/default/files/2022-02/CyberRiskToolkit.Feb22.pdf>
- Aon. (2021a). *Aon’s E&O | Cyber Insurance Snapshot* (p. 10). [https://library.cventia.com/report/report\\_007172.html](https://library.cventia.com/report/report_007172.html)
- Aon. (2021b). *US Cyber Market Update: 2020 US Cyber Insurance Profits And Performance* (p. 14). <http://thoughtleadership.aon.com/Documents/20210609-2021-cyber-market-update.pdf>
- Atluri, I. (2018). *Why Cyber Insurance Needs Probabilistic and Statistical Cyberrisk Assessments More Than Ever* (Volume 2; ISACA Journal, p. 10). <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-2/why-cyber-insurance-needs-probabilistic-and-statistical-cyberrisk-assessments-more-than-ever>
- Bean, M. (2020). *Exposure Measures for Pricing and Analyzing the Risks in Cyber Insurance* (p. 68). Casualty Actuarial Society and Society of Actuaries. <https://www.soa.org/49f336/globalassets/assets/files/resources/research-report/2020/exposure-measures-cyber-insurance.pdf>
- Bogomolny, O. (2017, January). *Cyber Insurance Conundrum: Using CIS Critical Security Controls for Underwriting Cyber Risk- A Masters Degree Candidate Presentation*. SANS Institute. <https://www.sans.org/webcasts/cyber-insurance-conundrum-cis-critical-security-controls-underwriting-cyber-risk-masters-degree-candidate-presentation-107015/>
- Cambridge Centre for Risk Studies. (2017). *2017 Cyber Risk Landscape* (p. 47). Cambridge Centre for Risk Studies at the University of Cambridge Judge Business School, in collaboration with Risk Management Solutions. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-rms-cyber-risk-landscape-2017.pdf>
- Cambridge Centre for Risk Studies. (2018). *Global Risk Index 2019 Executive Summary*. Cambridge Centre for Risk Studies, University of Cambridge. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-global-risk-index-exec-summary-2019.pdf>
- Cambridge Centre for Risk Studies. (2019). *Risk Management for the Consumer Sectors* (Cambridge Case Study Series, p. 48). Cambridge Centre for Risk Studies at the University of Cambridge Judge Business School, in collaboration with Institute of Risk Management. <https://www.jbs.cam.ac.uk/wp-content/uploads/2021/11/crs-risk-management-for-the-consumer-sectors.pdf>
- Cambridge Centre for Risk Studies. (2020). *Cyber Insurance Exposure Data Schema V1.0* (Cambridge Risk Framework Series, p. 19). Cambridge Centre for Risk Studies at the University of Cambridge Judge Business School. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-data-schema-v1.0.pdf>
- Carter, R. A., Pain, D., & Enoizi, J. (2022). *Insuring Hostile Cyber Activity: In search of sustainable solutions* (p. 48). The Geneva Association. [https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf\\_public/cybersolutions\\_web.pdf](https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cybersolutions_web.pdf)

- CISA. (2012). *Cybersecurity Insurance Workshop Readout Report*. <https://www.cisa.gov/sites/default/files/publications/November%202012%20Cybersecurity%20Insurance%20Workshop.pdf>
- CISA. (2013). *Cyber Risk Culture Roundtable Readout Report*. <https://www.cisa.gov/sites/default/files/publications/May%202013%20Cyber%20Risk%20Culture%20Roundtable.pdf>
- CISA. (2014a). *Cybersecurity Insurance Reports | CISA*. <https://www.cisa.gov/publication/cybersecurity-insurance-reports>
- CISA. (2014b). *Cyber Insurance Roundtable Readout Report—Health Care and Cyber Risk Management: Cost/Benefit Approaches* (p. 45). <https://www.cisa.gov/sites/default/files/publications/February%202014%20Cyber%20Insurance%20Health%20Care%20Use%20Case%20Roundtable.pdf>
- CISA. (2014c). *Insurance Industry Working Session Readout Report* (p. 49). [https://www.cisa.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session\\_1.pdf](https://www.cisa.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf)
- CISA. (2019). *Assessment of the Cyber Insurance Market*. [https://www.cisa.gov/sites/default/files/publications/19\\_1115\\_cisa\\_OCE-Cyber-Insurance-Market-Assessment.pdf](https://www.cisa.gov/sites/default/files/publications/19_1115_cisa_OCE-Cyber-Insurance-Market-Assessment.pdf)
- Citi GPS & Cambridge Centre for Risk Studies. (2021). *Systemic Risk: Systemic Solutions for an Increasingly Interconnected World* (p. 98). Citi GPS: Global Perspectives & Solutions and Centre for Risk Studies, University of Cambridge, Judge Business School. <https://www.jbs.cam.ac.uk/wp-content/uploads/2021/04/crs-citigps-systemic-risks-report.pdf>
- Coalition. (2021). *Cyber Insurance Claims Report: H1 2021* (p. 18). Cyentia Institute. <https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2020-09-Coalition-Cyber-Insurance-Claims-Report-2020.pdf>
- Coburn, A. W., Daffron, J., Quantrill, K., Leverett, É., Bordeau, J., Smith, A., & Harvey, T. (2019). *Cyber Risk Outlook*. Centre for Risk Studies, University of Cambridge, in collaboration with Risk Management Solutions, Inc. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-risk-outlook-2019.pdf>
- Coburn, A. W., Daffron, J., Smith, A., Bordeau, J., Leverett, É., Sweeney, S., & Harvey, T. (2018). *Cyber Risk Outlook*. Centre for Risk Studies, University of Cambridge, in collaboration with Risk Management Solutions, Inc. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-risk-outlook-2018.pdf>
- Corax & Clyde&Co. (2018). *2018 Cyber Breach Insights: Key Drivers Behind Cyber Insurance Claims* (p. 20). [https://library.cyentia.com/report/report\\_002913.html](https://library.cyentia.com/report/report_002913.html)
- Corix Partners & Cyber Solace. (2022). *Cyber Insurance: Changing Dynamics in a Maturing Market*. [https://library.cyentia.com/report/report\\_008822.html](https://library.cyentia.com/report/report_008822.html)
- Cowbell Cyber. (2022). *Cyber Round-Up Q2 2022*. <https://cowbell.insure/sme-cyber-round-up/>
- Cutler, J., Maxwell, L., Dionisi, S., Solomon, M., & Shang, K. (2017). *Cybersecurity: Impact on Insurance Business* (p. 20). Society of Actuaries. <https://www.soa.org/globalassets/assets/files/static-pages/sections/joint-risk-mgmt/cyber-security-impact.pdf>

- Cyber Risk Insurance Task Force, American Academy of Actuaries Casualty Practice Council. (2019). *Cyber Risk Insurance: A Resource Guide for Actuaries* (p. 16). <https://www.actuary.org/sites/default/files/2019-06/cyber-risk-insurance.pdf>
- Drouin, D. (2004). *Cyber Risk Insurance* (p. 29). SANS Institute. <https://www.sans.org/white-papers/1412/>
- Eling, M., & Schnell, W. (2016). *Ten Key Questions on Cyber Risk and Cyber Risk Insurance* (p. 88). The Geneva Association. [https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf\\_public/cyber-risk-10\\_key\\_questions.pdf](https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber-risk-10_key_questions.pdf)
- European Insurance and Occupational Pensions Authority. (2018). *Understanding Cyber Insurance—A Structured Dialogue with Insurance Companies* (p. 33). Publications Office of the European Union. <https://data.europa.eu/doi/10.2854/33407>
- European Insurance and Occupational Pensions Authority. (2020a). *Cyber risk for insurers- challenges and opportunities* (p. 30). Publications Office of the European Union. <https://doi.org/10.2854/305969>
- European Insurance and Occupational Pensions Authority. (2020b). *EIOPA Strategy on Cyber Underwriting* (p. 6). Publications Office. <https://data.europa.eu/doi/10.2854/793935>
- European Network and Information Security Agency. (2012). *Incentives and Barriers of the Cyber Insurance Market in Europe* (p. 45). <https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe>
- European Network and Information Security Agency. (2016). *Cyber insurance: Recent advances, good practices and challenges*. (p. 26). Publications Office of the European Union. <https://data.europa.eu/doi/10.2824/065381>
- European Network and Information Security Agency. (2017). *Commonality of risk assessment language in cyber insurance: Recommendations on cyber insurance*. (p. 52). Publications Office of the European Union. <https://data.europa.eu/doi/10.2824/691163>
- European Systemic Risk Board. (2020). *Systemic cyber risk*. Publications Office of the European Union. <https://data.europa.eu/doi/10.2849/566567>
- Evan, T., Leverett, É., Ruffle, S. J., Coburn, A. W., Bourdeau, J., Gunaratna, R., & Ralph, D. (2017). *Cyber Terrorism: Assessment of the Threat to Insurance* (Cambridge Risk Framework Series, p. 48). Centre for Risk Studies, University of Cambridge. <https://www.ibs.cam.ac.uk/wp-content/uploads/2020/08/pool-re-cyber-terrorism.pdf>
- Forscey, D., Bateman, J., Beecroft, N., & Woods, B. (2022). *Systemic Cyber Risk: A Primer* (p. 34). Carnegie Endowment for International Peace. <https://carnegieendowment.org/2022/03/07/systemic-cyber-risk-primer-pub-86531>
- Gallagher Re & Risk Management Solutions, Inc. (2022). *An Analytics-led Approach to Cyber Intelligence* (p. 3).
- Hall, D. (2020). *Exposure Measures for Pricing and Analyzing the Risks in Cyber Insurance Podcast*. Society of Actuaries. <https://www.soa.org/resources/research-reports/2020/exposure-measures-cyber-insurance/>
- Hartwig, R. P., & Wilkinson, C. (2015). *Cyber Risk: Threat and opportunity* (p. 33). Insurance Information Institute. [https://www.iii.org/sites/default/files/docs/pdf/cyber\\_risk\\_wp\\_final\\_102015.pdf](https://www.iii.org/sites/default/files/docs/pdf/cyber_risk_wp_final_102015.pdf)

- Hofmann, D. (2016). *Cyber insurance as a risk mitigation strategy* (p. 4). The Geneva Association. [https://cams.mit.edu/wp-content/uploads/research\\_brief\\_-\\_contours\\_of\\_an\\_emerging\\_market\\_for\\_cyber\\_risk\\_transfer.pdf](https://cams.mit.edu/wp-content/uploads/research_brief_-_contours_of_an_emerging_market_for_cyber_risk_transfer.pdf)
- Hofmann, D. M. (2018). *Advancing Accumulation Risk Management in Cyber Insurance* (p. 34). The Geneva Association. [https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf\\_public/report\\_advancing\\_accumulation\\_risk\\_management\\_in\\_cyber\\_insurance.pdf](https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/report_advancing_accumulation_risk_management_in_cyber_insurance.pdf)
- Howden. (2021). *Cyber Insurance: A Hard Reset* (p. 40). [https://library.cyentia.com/report/report\\_008129.html](https://library.cyentia.com/report/report_008129.html)
- Johansmeyer, T. (2021, January 11). Cybersecurity Insurance Has a Big Problem. *Harvard Business Review*. <https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem>
- Kaffenberger, L., & Kopp, E. (2019). *Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment* (p. 35). Carnegie Endowment for International Peace.
- Kelly, S., Leverett, É., Oughton, E. J., Copic, J., Thacker, S., Pant, R., Pryor, L., Kassara, G., Evan, T., Ruffle, S. J., Tuveson, M., Coburn, A. W., Ralph, D., & Hall, J. W. (2016). *Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy* (Cambridge Risk Framework Series). Centre for Risk Studies, University of Cambridge. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-integrated-infrastructure-cyber-resiliency-in-society.pdf>
- Liu, M. (2019). *A New Paradigm in Risk-Informed Cyber Insurance Policy Design: Meta-Policies and Risk Aggregation*. <https://apps.dtic.mil/sti/pdfs/AD1071891.pdf>
- Lloyd's. (2010). *Managing digital risk—Trends, issues and implications for business* (p. 52). <https://www.lloyds.com/news-and-insights/risk-reports/library/technology/managing-digital-risk>
- Lloyd's. (2015). *Business Blackout* (Innovation Series, p. 68). Centre for Risk Studies - University of Cambridge. <https://assets.lloyds.com/assets/pdf-business-blackout-business-blackout20150708/1/pdf-business-blackout-business-blackout20150708.pdf>
- Lloyd's. (2017a). *Stochastic modelling of liability accumulation risk* (p. 45). <https://assets.lloyds.com/assets/pdf-arium-stochastic-modelling/1/pdf-arium-stochastic-modelling.pdf>
- Lloyd's. (2017b). *Counting the cost—Cyber exposure decoded* (p. 56). <https://www.lloyds.com/news-and-insights/risk-reports/library/countingthecost>
- Lloyd's. (2018a). *Networked World—Risks and opportunities in the Internet of Things* (p. 73). <https://www.lloyds.com/news-and-insights/risk-reports/library/networked-world>
- Lloyd's. (2018b). *New Realities—Risks in the Virtual World* (p. 62). <https://www.lloyds.com/news-and-insights/risk-reports/library/new-realities>
- Lloyd's. (2019a). *Bashe Attack—Global infection by contagious malware* (p. 79). <https://www.lloyds.com/news-and-insights/risk-reports/library/bashe-attack>
- Lloyd's. (2019b). *Taking Control—Artificial intelligence and insurance* (p. 61). <https://www.lloyds.com/news-and-insights/risk-reports/library/taking-control>
- Lloyd's. (2019c). *Shen Attack—Cyber Risk In Asia Pacific Ports* (p. 85). <https://www.lloyds.com/news-and-insights/risk-reports/library/shen-attack-cyber-risk-in-asia-pacific-ports>

Lloyd's. (2020a). *Protecting intangible assets: Preparing for a new reality* (p. 45). <https://www.lloyds.com/news-and-insights/risk-reports/library/lloyds-intangibles>

Lloyd's. (2020b). *Building simpler insurance products to better protect customers* (p. 30). <https://www.lloyds.com/news-and-insights/market-communications/covid-19/lloyds-covid19-response-package/building-simpler-insurance-products-to-better-protect-customers>

Lloyd's. (2020c). *Cities at risk – Building a resilient future for the world's urban centres* (p. 93). <https://www.lloyds.com/news-and-insights/risk-reports/library/cities-at-risk>

Lloyd's. (2020d). *Data puts active portfolio management on a firm footing* (p. 48). <https://www.lloyds.com/news-and-insights/risk-reports/library/data-puts-active-portfolio-management-on-a-firm-footing>

Lloyd's. (2020e). *Safeguarding reputation* (p. 24). <https://www.lloyds.com/news-and-insights/risk-reports/library/safeguarding-reputation>

Lloyd's. (2021a). *Cyber risk: The emerging cyber threat to industrial control systems*. <https://www.lloyds.com/news-and-insights/risk-reports/library/icsreport>

Lloyd's. (2021b). *Cyber risk in Aviation*. <https://www.lloyds.com/news-and-insights/risk-reports/library/cyber-risk-in-aviation>

MacColl, J., Nurse, J. R. C., & Sullivan, J. (2021). *Cyber Insurance and the Cyber Security Challenge* (RUSI Occasional Paper, p. 68). Royal United Services Institute for Defence and Security Studies. <https://static.rusi.org/247-op-cyber-insurance-v2.pdf>

Marciano, C. (2020, April 25). *How much does Cyber Insurance Cost? Cyber Insurance | Data Breach Insurance Premiums*. Data Breach Insurance. <https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums/>

Marsh. (2020a). *Global Insurance Pricing Continues to Increase in First Quarter 2020*. <https://www.marsh.com/uk/services/international-placement-services/insights/global-insurance-pricing-continues-to-increase-in-first-quarter-2020.html>

Marsh. (2020b). *Silent Cyber: Managing Cyber Coverage within a Changing Insurance Market*. <https://www.marsh.com/uk/services/cyber-risk/insights/silent-cyber-managing-coverage-in-changing-insurance-market.html>

Marsh. (2020c). *Writing Clear Contracts for Cyber Risk Transfer*. <https://www.marsh.com/uk/services/cyber-risk/insights/writing-contracts-cyber-risk-transfer.html>

Marsh. (2022). *Global Insurance Market Index—2022 Q1*. [https://info.marsh.com/l/395202/2022-04-26/c769hd/395202/16509910878h7JyNnA/GIMI\\_Q1\\_2022\\_report.pdf](https://info.marsh.com/l/395202/2022-04-26/c769hd/395202/16509910878h7JyNnA/GIMI_Q1_2022_report.pdf)

Marsh McLennan. (2020). *MMC Cyber Handbook 2021* (p. 59). [https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2020/october/MMC\\_Cyber\\_Handbook\\_2021.pdf](https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2020/october/MMC_Cyber_Handbook_2021.pdf)

NAIC. (2021). *Report on the Cybersecurity Insurance Market* (p. 7). [https://content.naic.org/sites/default/files/index-cmte-c-Cyber\\_Supplement\\_2020\\_Report.pdf](https://content.naic.org/sites/default/files/index-cmte-c-Cyber_Supplement_2020_Report.pdf)

National Institute of Standards and Technology. (2020). *NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0* (NIST CSWP 01162020; p. NIST CSWP 01162020). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.CSWP.01162020>

NetDiligence. (2021). *Cyber Claims Study: 2021 Report* (p. 53). [https://library.cyentia.com/report/report\\_008228.html](https://library.cyentia.com/report/report_008228.html)

O'Brien, S., Platt, J. S., Davis, E., Shafer, C., Bole, R., & Essen, Y. (2020). *Looking Beyond the Clouds: A U.S. Cyber Insurance Industry Catastrophe Loss Study* (p. 28). Marsh McLennan. <https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2020/october/Beyond-the-Clouds.pdf>

OECD. (2017a). *Supporting an Effective Cyber Insurance Market—OECD Report for the G7 Presidency* (p. 20). <https://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf>

OECD. (2017b). *Enhancing the Role of Insurance in Cyber Risk Management*. OECD. <https://doi.org/10.1787/9789264282148-en>

OECD. (2017c). The cyber insurance market: Responding to a risk with few boundaries. In *Enhancing the Role of Insurance in Cyber Risk Management* (p. 4). OECD. <https://doi.org/10.1787/9789264282148-en>

OECD. (2018). *Unleashing the Potential of the Cyber Insurance Market—Conference Outcomes* (p. 30). <https://www.oecd.org/daf/fin/insurance/Unleashing-Potential-Cyber-Insurance-Market-Summary.pdf>

OECD. (2020a). *Encouraging Clarity in Cyber Insurance Coverage* (p. 42). OECD. <https://www.oecd.org/daf/fin/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf>

OECD. (2020b). *Enhancing the Availability of Data for Cyber Insurance Underwriting* (p. 15). <https://www.oecd.org/daf/fin/insurance/Enhancing-the-Availability-of-Data-for-Cyber-Insurance-Underwriting.pdf>

OECD. (2020c). *Insurance Coverage for Cyber Terrorism in Australia*. <https://www.oecd.org/finance/insurance/Insurance-Coverage-for-Cyber-Terrorism-in-Australia.htm>

QOMPLX. (2020). *Mind the Gap: The Underinsurance of Cyber Risk* (p. 12). [https://library.cyentia.com/report/report\\_003468.html](https://library.cyentia.com/report/report_003468.html)

Reagan, T., Schnur, M., Parisi, B., & Corrado, J. (2020). *Cyber Insurance Purchasing Grows Again in 2019* (p. 8). Marsh McLennan. <https://www.marshmclennan.com/content/dam/marsh/Documents/PDF/US-en/cyber-insurance-purchasing-report.pdf>

*Risk Centre publications*. (n.d.). Cambridge Judge Business School. Retrieved June 23, 2022, from <https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/>

Risk Management Solutions, Inc. (2016). *Managing Cyber Insurance Accumulation Risk* (p. 65). Report prepared in collaboration with and based on original research by the Centre for Risk Studies, University of Cambridge. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-rms-managing-cyber-insurance-accumulation-risk.pdf>

Romanosky, S. (2017). *Content Analysis of Cyber Insurance Policies: How do carriers write policies and price cyber risk?* (p. 40). [https://www.ftc.gov/system/files/documents/public\\_comments/2017/10/00012-141437.pdf](https://www.ftc.gov/system/files/documents/public_comments/2017/10/00012-141437.pdf)

Ruffle, S. J., Bowman, G., Caccioli, F., Coburn, A. W., Kelly, S., Leslie, B., & Ralph, D. (2014). *Stress Test Scenario: Sybil Logic Bomb Cyber Catastrophe* (Cambridge Risk Framework Series, p. 45). Centre for Risk Studies, University of

Cambridge. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-sybil-logic-bomb-cyber-catastrophe-stress-test.pdf>

Sullivan, J., & Nurse, J. R. C. (2020). *Cyber Security Incentives and the Role of Cyber Insurance* (Emerging Insights, p. 20). Royal United Services Institute for Defence and Security Studies. [https://static.rusi.org/246\\_ei\\_cyber\\_insurance\\_final\\_web\\_version.pdf](https://static.rusi.org/246_ei_cyber_insurance_final_web_version.pdf)

Tatar, U., Keskin, O., Bahsi, H., & Pinto, C. A. (2020). *Quantification of Cyber Risk for Actuaries An Economic-Functional Approach* (p. 84). Society of Actuaries. <https://www.soa.org/49c222/globalassets/assets/files/resources/research-report/2020/quantification-cyber-risk.pdf>

*The VERIS Framework*. (2013). <http://veriscommunity.net/>

Tracy, R. (2019, July 10). *Could NIST SP 800-171 Be A Model for the Cyber Insurance Industry?* Telos Corporation. <https://www.telos.com/blog/2019/07/10/nist-800-171b-cyber-insurance/>

U. S. Government Accountability Office. (2021). *Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market* (GAO-21-477; p. 26). <https://www.gao.gov/products/gao-21-477>

U. S. Government Accountability Office. (2022). *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks* (GAO-22-104256; p. 53). <https://www.gao.gov/assets/gao-22-104256.pdf>

U.S. Cyberspace Solarium Commission. (2020). *The Cyberspace Solarium Commission report: A warning from tomorrow* (p. 182).

Willis Tower Watson. (2020). *Cyber Claims Analysis Report*. <https://www.willistowerswatson.com/-/media/WTW/Insights/2020/07/cyber-claims-analysis-report.pdf>

Wolfrom, L. (2020). *Building a Sustainable Cyber Insurance Market* (p. 4). <https://www.oecd.org/daf/fin/insurance/Building-a-Sustainable-Cyber-Insurance-Market.pdf>

World Economic Forum. (2022). *The Global Risks Report 2022* (Insight Report, p. 117). World Economic Forum, Marsh McLennan, SK Group, and Zurich Insurance Group. <https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2022/global-risks-report-2022/global-risks-report-2022.pdf>

Zhang, X., Xu, M., & Su, J. (2021). *Modeling and Pricing Cybersecurity Risks in Fog Computing Based IoT Architectures* (p. 37). Society of Actuaries. <https://www.soa.org/resources/research-reports/2021/cybersecurity-risks/>



## References – Academic Literature

- Acharya, S., Mieth, R., Konstantinou, C., Karri, R., & Dvorkin, Y. (2021). Cyber Insurance Against Cyberattacks on Electric Vehicle Charging Stations. *IEEE Transactions on Smart Grid*, 1–1. <https://doi.org/10.1109/TSG.2021.3133536>
- Aditya, K., Grzonkowski, S., & Le-Khac, N.-A. (2018). RiskWriter: Predicting Cyber Risk of an Enterprise. In V. Ganapathy, T. Jaeger, & R. K. Shyamasundar (Eds.), *Information Systems Security* (pp. 88–106). Springer International Publishing. [https://doi.org/10.1007/978-3-030-05171-6\\_5](https://doi.org/10.1007/978-3-030-05171-6_5)
- Antonio, Y., Indratno, S., & Simanjuntak, R. (2021). Cyber Insurance Ratemaking: A Graph Mining Approach. *Risks*, 9(12). <https://doi.org/10.3390/risks9120224>
- Antonio, Y., Indratno, S. W., & Saputro, S. W. (2021). Pricing of cyber insurance premiums using a Markov-based dynamic model with clustering structure. *PLOS ONE*, 16(10), e0258867. <https://doi.org/10.1371/journal.pone.0258867>
- Awiszus, K., Knispel, T., Penner, I., Svindland, G., Voß, A., & Weber, S. (2022). Modeling and Pricing Cyber Insurance – A Survey. 35.
- Bandyopadhyay, T., & Mookerjee, V. (2019). A model to analyze the challenge of using cyber insurance. *Information Systems Frontiers*, 21(2), 301–325. <https://doi.org/10.1007/s10796-017-9737-3>
- Barreto, C., Cardenas, A. A., & Schwartz, G. (2018). Cyber-Insurance for Cyber-Physical Systems. 2018 IEEE Conference on Control Technology and Applications (CCTA), 1704–1711. <https://doi.org/10.1109/CCTA.2018.8511535>
- Bessy-Roland, Y., Boumezoued, A., & Hillairet, C. (2021). Multivariate Hawkes process for cyber insurance. *Annals of Actuarial Science*, 15(1), 14–39. <https://doi.org/10.1017/S1748499520000093>
- Bodin, L., Gordon, L., Loeb, M., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, 37(6), 527–544. <https://doi.org/10.1016/j.jaccpubpol.2018.10.004>
- Böhme, R., & Kataria, G. (2006). On the Limits of Cyber-Insurance. In S. Fischer-Hübner, S. Furnell, & C. Lambrinouidakis (Eds.), *Trust and Privacy in Digital Business* (pp. 31–40). Springer. [https://doi.org/10.1007/11824633\\_4](https://doi.org/10.1007/11824633_4)
- Böhme, R., Laube, S., & Riek, M. (2019). *A Fundamental Approach to Cyber Risk Analysis*. 12(2), 25. [https://informationsecurity.uibk.ac.at/pdfs/BLR2019\\_FundamentalApproachCyberRiskInsurance\\_Variance.pdf](https://informationsecurity.uibk.ac.at/pdfs/BLR2019_FundamentalApproachCyberRiskInsurance_Variance.pdf)
- Carannante, M., D’Amato, V., Forte, S., Fersini, P., & Melisi, G. (2022). Vine Copula Modelling Dependence Among Cyber Risks: A Dangerous Regulatory Paradox (SSRN Scholarly Paper No. 4041750). Social Science Research Network. <https://doi.org/10.2139/ssrn.4041750>
- Carfora, M. F., & Orlando, A. (2019). Quantile based risk measures in cyber security. 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 1–4. <https://doi.org/10.1109/CyberSA.2019.8899431>
- Carfora, M. F., & Orlando, A. (2022). Cyber Risk: Estimates for Malicious and Negligent Breaches Distributions. In M. Corazza, C. Perna, C. Pizzi, & M. Sibillo (Eds.), *Mathematical and Statistical Methods for Actuarial Sciences and Finance* (pp. 140–145). Springer International Publishing. [https://doi.org/10.1007/978-3-030-99638-3\\_23](https://doi.org/10.1007/978-3-030-99638-3_23)
- Carfora, M., Martinelli, F., Mercaldo, F., & Orlando, A. (2019). Cyber risk management: An actuarial point of view. *Journal of Operational Risk*, 14(4), 77–103. <https://doi.org/10.21314/JOP.2019.231>



- Egan, R., Cartagena, S., Mohamed, R., Gosrani, V., Grewal, J., Acharyya, M., Dee, A., Bajaj, R., Jaeger, V.-J., Katz, D., Meghen, P., Silley, M., Nasser-Probert, S., Pikinska, J., Rubin, R., & Ang, K. (2019). Cyber operational risk scenarios for insurance companies. *British Actuarial Journal*, 24. <https://doi.org/10.1017/S1357321718000284>
- Eling, M., Elvedi, M., & Falco, G. (2022). The Economic Impact of Extreme Cyber Risk Scenarios. *North American Actuarial Journal*, 0(0), 1–15. <https://doi.org/10.1080/10920277.2022.2034507>
- Eling, M., & Jung, K. (2018). Copula approaches for modeling cross-sectional dependence of data breach losses. *Insurance: Mathematics and Economics*, 82, 167–180. <https://doi.org/10.1016/j.insmatheco.2018.07.003>
- Eling, M., & Jung, K. (2022). Heterogeneity in cyber loss severity and its impact on cyber risk measurement. *Risk Management*. <https://doi.org/10.1057/s41283-022-00095-w>
- Eling, M., Jung, K., & Shim, J. (2022). Unraveling heterogeneity in cyber risks using quantile regressions. *Insurance: Mathematics and Economics*, 104, 222–242. <https://doi.org/10.1016/j.insmatheco.2022.03.001>
- Eling, M., & Loperfido, N. (2017). Data breaches: Goodness of fit, pricing, and risk measurement. *Insurance: Mathematics and Economics*, 75, 126–136. <https://doi.org/10.1016/j.insmatheco.2017.05.008>
- Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, 272(3), 1109–1119. <https://doi.org/10.1016/j.ejor.2018.07.021>
- Erdogan, G., Gonzalez, A., Refsdal, A., & Seehusen, F. (2017). A Method for Developing Algorithms for Assessing Cyber-Risk Cost. 2017 IEEE International Conference on Software Quality, Reliability and Security (QRS), 192–199. <https://doi.org/10.1109/QRS.2017.29>
- Erola, A., Agrafiotis, I., Nurse, J. R. C., Axon, L., Goldsmith, M., & Creese, S. (2022). A system to calculate Cyber Value-at-Risk. *Computers & Security*, 113, 102545. <https://doi.org/10.1016/j.cose.2021.102545>
- Fahrenwaldt, M., Weber, S., & Weske, K. (2018). Pricing of Cyber Insurance Contracts in a Network Model. *Astin Bulletin*, 48(3), 1175–1218. <https://doi.org/10.1017/asb.2018.23>
- Farkas, S., Lopez, O., & Thomas, M. (2021). Cyber claim analysis using Generalized Pareto regression trees with applications to insurance. *Insurance: Mathematics and Economics*, 98, 92–105. <https://doi.org/10.1016/j.insmatheco.2021.02.009>
- Feng, S., Wang, W., Xiong, Z., Niyato, D., Wang, P., & S. S. Wang. (2021). On Cyber Risk Management of Blockchain Networks: A Game Theoretic Approach. *IEEE Transactions on Services Computing*, 14(5), 1492–1504. <https://doi.org/10.1109/TSC.2018.2876846>
- Feng, S., Xiong, Z., Niyato, D., & Wang, P. (2018). Competitive Security Pricing in Cyber-Insurance Market: A Game-Theoretic Analysis. 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), 1–5. <https://doi.org/10.1109/VTCFall.2018.8690762>
- Feng, S., Xiong, Z., Niyato, D., & Wang, P. (2021). Dynamic Resource Management to Defend Against Advanced Persistent Threats in Fog Computing: A Game Theoretic Approach. *IEEE Transactions on Cloud Computing*, 9(3), 995–1007. <https://doi.org/10.1109/TCC.2019.2896632>
- Franke, U., & Draeger, J. (2019). Two simple models of business interruption accumulation risk in cyber insurance. 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 1–7. <https://doi.org/10.1109/CyberSA.2019.8899678>

Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance*, n/a(n/a).

<https://doi.org/10.1111/jori.12381>

Hayel, Y., & Zhu, Q. (2015). Attack-Aware Cyber Insurance for Risk Sharing in Computer Networks (M. Khouzani, E. Panaousis, & G. Theodorakopoulos, Eds.; WOS:000374103200002; Vol. 9406, pp. 22–34).

[https://doi.org/10.1007/978-3-319-25594-1\\_2](https://doi.org/10.1007/978-3-319-25594-1_2)

Hillairet, C., & Lopez, O. (2021). Propagation of cyber incidents in an insurance portfolio: Counting processes combined with compartmental epidemiological models. *Scandinavian Actuarial Journal*, 2021(8), 671–694.

<https://doi.org/10.1080/03461238.2021.1872694>

Hua, L., & Xu, M. (2021). Pricing Cyber Insurance for a Large-Scale Network. *Variance*, 14(2), 19.

Insua, D., Couce-Vieira, A., & Musaraj, K. (2018). Some Risk Analysis Problems in Cyber Insurance Economics. *Estudios De Economia Aplicada*, 36(1), 181–194.

Insua, D., Couce-Vieira, A., Rubio, J., Pieters, W., Labunets, K., & Rasines, D. (2021). An Adversarial Risk Analysis Framework for Cybersecurity. *Risk Analysis*, 41(1), 16–36. <https://doi.org/10.1111/risa.13331>

Jevtić, P., & Lanchier, N. (2020). Dynamic structural percolation model of loss distribution for cyber risk of small and medium-sized enterprises for tree-based LAN topology. *Insurance: Mathematics and Economics*, 91, 209–223.

<https://doi.org/10.1016/j.insmatheco.2020.02.005>

Johnson, B., Laszka, A., & Grossklags, J. (2014). How Many down? Toward Understanding Systematic Risk in Networks. *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, 495–500. <https://doi.org/10.1145/2590296.2590308>

Jung, K. (2021). Extreme Data Breach Losses: An Alternative Approach to Estimating Probable Maximum Loss for Data Breach Risk. *North American Actuarial Journal*, 25(4), 580–603.

<https://doi.org/10.1080/10920277.2021.1919145>

Kelliher, P. O. J., Acharyya, M., Couper, A., Grant, K., Maguire, E., Nicholas, P., Smerald, C., Stevenson, D., Thirlwell, J., & Cantle, N. (2017). Good practice guide to setting inputs for operational risk models. *British Actuarial Journal*, 22(1), 68–108. <https://doi.org/10.1017/S1357321716000179>

Khalili, M., Liu, M., & Romanosky, S. (2019). Embracing and controlling risk dependency in cyber-insurance policy underwriting. *Journal of Cybersecurity*, 5(1). <https://doi.org/10.1093/cybsec/tyz010>

Khalili, M. M., Naghizadeh, P., & Liu, M. (2017). Embracing Risk Dependency in Designing Cyber-Insurance Contracts. 2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton), 926–933.

<https://doi.org/10.1109/ALLERTON.2017.8262837>

Khalili, M. M., Naghizadeh, P., & Liu, M. (2018). Designing Cyber Insurance Policies: The Role of Pre-Screening and Security Interdependence. *IEEE Transactions on Information Forensics and Security*, 13(9), 2226–2239.

<https://doi.org/10.1109/TIFS.2018.2812205>

Khalili, M. M., Zhang, X., & Liu, M. (2019). Effective Premium Discrimination for Designing Cyber Insurance Policies with Rare Losses. In T. Alpcan, Y. Vorobeychik, J. S. Baras, & G. Dán (Eds.), *Decision and Game Theory for Security* (pp. 259–275). Springer International Publishing. [https://doi.org/10.1007/978-3-030-32430-8\\_16](https://doi.org/10.1007/978-3-030-32430-8_16)

- Laszka, A., Johnson, B., & Grossklags, J. (2018). On the Assessment of Systematic Risk in Networked Systems. *ACM Trans. Internet Technol.*, 18(4). <https://doi.org/10.1145/3166069>
- Laszka, A., Johnson, B., Grossklags, J., & Felegyhazi, M. (2014). Estimating Systematic Risk in Real-World Networks. In N. Christin & R. Safavi-Naini (Eds.), *Financial Cryptography and Data Security* (pp. 417–435). Springer. [https://doi.org/10.1007/978-3-662-45472-5\\_27](https://doi.org/10.1007/978-3-662-45472-5_27)
- Lau, P., Wang, L., Liu, Z., Wei, W., & Ten, C.-W. (2021). A Coalitional Cyber-Insurance Design Considering Power System Reliability and Cyber Vulnerability. *IEEE Transactions on Power Systems*, 36(6), 5512–5524. <https://doi.org/10.1109/TPWRS.2021.3078730>
- Lau, P., Wang, L., Wei, W., Liu, Z., & Ten, C.-W. (2022). A Novel Mutual Insurance Model for Hedging Against Cyber Risks in Power Systems Deploying Smart Technologies. *IEEE Transactions on Power Systems*, 1–1. <https://doi.org/10.1109/TPWRS.2022.3164628>
- Li, J., Niyato, D., Hong, C. S., Park, K.-J., Wang, L., & Han, Z. (2020). A Contract-Theoretic Cyber Insurance for Withdraw Delay in the Blockchain Networks with Shards. *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 1–7. <https://doi.org/10.1109/ICC40277.2020.9149437>
- Lin, Z., Sapp, T. R. A., Parsa, R., Ulmer, J. R., & Cao, C. (2021). Pricing Cyber Security Insurance. *Journal of Mathematical Finance*, 12(1), 46–70. <https://doi.org/10.4236/jmf.2022.121003>
- Liu, J., Li, J., & Daly, K. (2022). Bayesian vine copulas for modelling dependence in data breach losses. *Annals of Actuarial Science*, 1–24. <https://doi.org/10.1017/S174849952200001X>
- Liu, M. (2021). Embracing Risk: Cyber Insurance as an Incentive Mechanism for Cybersecurity. *Morgan & Claypool*. <https://doi.org/10.2200/S01093ED1V01Y202104LNA026>
- Liu, Z., Wei, W., & Wang, L. (2021). An Extreme Value Theory Based Catastrophe Bond Design for Cyber Risk Management of Power Systems. *IEEE Transactions on Smart Grid*, 1–1. <https://doi.org/10.1109/TSG.2021.3131468>
- Liu, Z., Wei, W., Wang, L., Ten, C.-W., & Rho, Y. (2021). An Actuarial Framework for Power System Reliability Considering Cybersecurity Threats. *IEEE Transactions on Power Systems*, 36(2), 851–864. <https://doi.org/10.1109/TPWRS.2020.3018701>
- Lu, X., Niyato, D., Jiang, H., Wang, P., & Poor, H. V. (2018). Cyber Insurance for Heterogeneous Wireless Networks. *IEEE Communications Magazine*, 56(6), 21–27. <https://doi.org/10.1109/MCOM.2018.1700504>
- Meland, P. H., & Seehusen, F. (2018). When to Treat Security Risks with Cyber Insurance. *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–8. <https://doi.org/10.1109/CyberSA.2018.8551456>
- Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. *Information Systems Frontiers*, 21(5), 997–1018. <https://doi.org/10.1007/s10796-017-9808-5>
- Pal, R., & Golubchik, L. (2010). On the Economics of Information Security: The Problem of Designing Optimal Cyber-Insurance Contracts. *SIGMETRICS Perform. Eval. Rev.*, 38(2), 51–53. <https://doi.org/10.1145/1870178.1870196>
- Pal, R., Golubchik, L., Psounis, K., & Bandyopadhyay, T. (2019). On Robust Estimates of Correlated Risk in Cyber-Insured IT Firms: A First Look at Optimal AI-Based Estimates under “Small” Data. *ACM Trans. Manage. Inf. Syst.*, 10(3). <https://doi.org/10.1145/3351158>

- Pal, R., Golubchik, L., Psounis, K., & Hui, P. (2019). Security Pricing as Enabler of Cyber-Insurance A First Look at Differentiated Pricing Markets. *IEEE Transactions on Dependable and Secure Computing*, 16(2), 358–372. <https://doi.org/10.1109/TDSC.2017.2684801>
- Pal, R., Huang, Z., Yin, X., Lototsky, S., De, S., Tarkoma, S., Liu, M., Crowcroft, J., & Sastry, N. (2021). Aggregate Cyber-Risk Management in the IoT Age: Cautionary Statistics for (Re)Insurers and Likes. *IEEE Internet of Things Journal*, 8(9), 7360–7371. <https://doi.org/10.1109/JIOT.2020.3039254>
- Pal, R., & Hui, P. (2012). CyberInsurance for Cybersecurity a Topological Take on Modulating Insurance Premiums. *SIGMETRICS Perform. Eval. Rev.*, 40(3), 86–88. <https://doi.org/10.1145/2425248.2425271>
- Palsson, K., Gudmundsson, S., & Shetty, S. (2020). Analysis of the impact of cyber events for cyber insurance. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 45(4), 564–579. <https://doi.org/10.1057/s41288-020-00171-w>
- Pate-Cornell, M.-E., & Kuypers, M. A. (2021). A Probabilistic Analysis of Cyber Risks. *IEEE Transactions on Engineering Management*, 1–11. <https://doi.org/10.1109/TEM.2020.3028526>
- Piromsopa, K., Klima, T., & Pavlik, L. (2017). Designing Model for Calculating the Amount of Cyber Risk Insurance. 2017 Fourth International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), 196–200. <https://doi.org/10.1109/MCSI.2017.41>
- Pooser, D. M., Browne, M. J., & Arkhangelska, O. (2018). Growth in the Perception of Cyber Risk: Evidence from U.S. P&C Insurers. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 43(2), 208–223. <https://doi.org/10.1057/s41288-017-0077-9>
- Poyraz, O. I., Canan, M., McShane, M., Pinto, C. A., & Cotter, T. S. (2020). Cyber assets at risk: Monetary impact of U.S. personally identifiable information mega data breaches. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 45(4), 616–638. <https://doi.org/10.1057/s41288-020-00185-4>
- Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, 5(1). <https://doi.org/10.1093/cybsec/tyz002>
- Saini, D., Azad, I., Raut, N., & Hadimani, L. (2011). Utility Implementation for Cyber Risk Insurance Modeling (S. Ao, L. Gelman, D. Hukins, A. Hunter, & A. Korsunsky, Eds.; WOS:000393011100086; pp. 429–432).
- Schwartz, G. A., & Sastry, S. S. (2014). Cyber-Insurance Framework for Large Scale Interdependent Networks. *Proceedings of the 3rd International Conference on High Confidence Networked Systems*, 145–154. <https://doi.org/10.1145/2566468.2566481>
- Shah, A., Dahake, S., & J., S. H. H. (2015). Valuing Data Security and Privacy Using Cyber Insurance. *SIGCAS Comput. Soc.*, 45(1), 38–41. <https://doi.org/10.1145/2738210.2738217>
- Sharma, K., & Mukhopadhyay, A. (2022a). Cyber-risk Management Framework for Online Gaming Firms: An Artificial Neural Network Approach. *Information Systems Frontiers*. <https://doi.org/10.1007/s10796-021-10232-7>
- Sharma, K., & Mukhopadhyay, A. (2022b). Sarima-Based Cyber-Risk Assessment and Mitigation Model for A Smart City's Traffic Management Systems (Scram). *Journal of Organizational Computing and Electronic Commerce*, 0(0), 1–20. <https://doi.org/10.1080/10919392.2022.2054259>
- Sheehan, B., Murphy, F., Kia, A. N., & Kiely, R. (2021). A quantitative bow-tie cyber risk classification and assessment framework. *Journal of Risk Research*, 24(12), 1619–1638. <https://doi.org/10.1080/13669877.2021.1900337>

- Shetty, N., Schwartz, G., Felegyhazi, M., & Walrand, J. (2010). Competitive Cyber-Insurance and Internet Security. In T. Moore, D. Pym, & C. Ioannidis (Eds.), *Economics of Information Security and Privacy* (pp. 229–247). Springer US. [https://doi.org/10.1007/978-1-4419-6967-5\\_12](https://doi.org/10.1007/978-1-4419-6967-5_12)
- Shetty, S., McShane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K., & Njilla, L. L. (2018). Reducing Informational Disadvantages to Improve Cyber Risk Management†. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 43(2), 224–238. <https://doi.org/10.1057/s41288-018-0078-3>
- Skeoch, H. R. K. (2022). Expanding the Gordon-Loeb model to cyber-insurance. *Computers & Security*, 112, 102533. <https://doi.org/10.1016/j.cose.2021.102533>
- Strupczewski, G. (2019). What Is the Worst Scenario? Modeling Extreme Cyber Losses. In P. Linsley, P. Shrives, & M. Wieczorek-Kosmala (Eds.), *Multiple Perspectives in Risk and Risk Management* (pp. 211–230). Springer International Publishing. [https://doi.org/10.1007/978-3-030-16045-6\\_10](https://doi.org/10.1007/978-3-030-16045-6_10)
- Sun, H., Xu, M., & Zhao, P. (2021). Modeling Malicious Hacking Data Breach Risks. *North American Actuarial Journal*, 25(4), 484–502. <https://doi.org/10.1080/10920277.2020.1752255>
- Uuganbayar, G., Massacci, F., Yautsiukhin, A., & Martinelli, F. (2019). Cyber Insurance and Time-to-Compromise: An Integrated Approach. 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), 1–8. <https://doi.org/10.1109/CyberSA.2019.8899442>
- Vakilinia, I., & Sengupta, S. (2019). A Coalitional Cyber-Insurance Framework for a Common Platform. *IEEE Transactions on Information Forensics and Security*, 14(6), 1526–1538. <https://doi.org/10.1109/TIFS.2018.2881694>
- Verlaine, M. (2021). On the extraction of cyber risks from structured products. *Applied Economics*. <https://doi.org/10.1080/00036846.2021.1998327>
- Wang, L., Iyengar, S. S., Belman, A. K., Phoha, V. V., & Wan, C. (2021). Game Theory Based Cyber-Insurance to Cover Potential Loss from Mobile Malware Exploitation. *Digital Threats: Research and Practice*, 2(2). <https://doi.org/10.1145/3409959>
- Wang, S., & Franke, U. (2020). Enterprise IT service downtime cost and risk transfer in a supply chain. *Operations Management Research*, 13(1–2), 94–108. <https://doi.org/10.1007/s12063-020-00148-x>
- Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, 57, 101173. <https://doi.org/10.1016/j.pacfin.2019.101173>
- Watson, T. F., Thakur, K., & Ali, M. L. (2022). The Impact of Purchasing Cyber Insurance on the Enhancement of Operational Cyber Risk Mitigation of U.S. Banks—A Case Study. 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 0709–0715. <https://doi.org/10.1109/CCWC54503.2022.9720791>
- Welburn, J., & Strong, A. (2021). Systemic Cyber Risk and Aggregate Impacts. *Risk Analysis*. <https://doi.org/10.1111/risa.13715>
- Woods, D. W., Moore, T., & Simpson, A. C. (2021). The County Fair Cyber Loss Distribution: Drawing Inferences from Insurance Prices. *Digital Threats: Research and Practice*, 2(2). <https://doi.org/10.1145/3434403>
- Xie, X., Lee, C., & Eling, M. (2020). Cyber insurance offering and performance: An analysis of the U.S. cyber insurance market. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 45(4), 690–736. <https://doi.org/10.1057/s41288-020-00176-5>

- Xu, M., & Hua, L. (2019). Cybersecurity Insurance: Modeling and Pricing. *North American Actuarial Journal*, 23(2), 220–249. <https://doi.org/10.1080/10920277.2019.1566076>
- Xu, M., & Zhang, Y. (2021). Data Breach CAT Bonds: Modeling and Pricing. *North American Actuarial Journal*, 25(4), 543–561. <https://doi.org/10.1080/10920277.2021.1886948>
- Yang, Y., Ji, G., Yang, Z., & Xue, S. (2019). Incentive Contract for Cybersecurity Information Sharing Considering Monitoring Signals. 2019 International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 507–512. <https://doi.org/10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00103>
- Yang, Y., Yang, Q., Yang, Z., & Xue, S. (2019). Optimal Model Design for the Cyber-Insurance Contract with Asymmetric Information. 2019 International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 513–518. <https://doi.org/10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00104>
- Yang, Z., Liu, Y., Campbell, M., Ten, C.-W., Rho, Y., Wang, L., & Wei, W. (2020). Premium Calculation for Insurance Businesses Based on Cyber Risks in IP-Based Power Substations. *IEEE Access*, 8, 78890–78900. <https://doi.org/10.1109/ACCESS.2020.2988548>
- Young, D., Lopez, J., Rice, M., Ramsey, B., & McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, 14, 43–57. <https://doi.org/10.1016/j.ijcip.2016.04.001>
- Zeller, G., & Scherer, M. (2021). A comprehensive model for cyber risk based on marked point processes and its application to insurance. *European Actuarial Journal*. <https://doi.org/10.1007/s13385-021-00290-1>
- Zhang, R., & Zhu, Q. (2020). FlipIn: A Game-Theoretic Cyber Insurance Framework for Incentive-Compatible Cyber Risk Management of Internet of Things. *IEEE Transactions on Information Forensics and Security*, 15, 2026–2041. <https://doi.org/10.1109/TIFS.2019.2955891>
- Zhang, R., & Zhu, Q. (2021). Optimal Cyber-Insurance Contract Design for Dynamic Risk Management and Mitigation. *IEEE Transactions on Computational Social Systems*, 1–14. <https://doi.org/10.1109/TCSS.2021.3117905>
- Zhang, R., Zhu, Q., & Hayel, Y. (2017). A Bi-Level Game Approach to Attack-Aware Cyber Insurance of Computer Networks. *IEEE Journal on Selected Areas in Communications*, 35(3), 779–794. <https://doi.org/10.1109/JSAC.2017.2672378>
- Zhang, Y., Wang, L., Liu, Z., & Wei, W. (2021). A Cyber-Insurance Scheme for Water Distribution Systems Considering Malicious Cyberattacks. *IEEE Transactions on Information Forensics and Security*, 16, 1855–1867. <https://doi.org/10.1109/TIFS.2020.3045902>

## References – Other

- Adamczyk, D. (2022, March 8). Ransomware's Impact on Cyber Insurance. *RSA Conference*. <http://www.rsaconference.com/library/blog/ransoms-impact-on-cyber-insurance>
- Atluri, I. (2018). *Why Cyber Insurance Needs Probabilistic and Statistical Cyberrisk Assessments More Than Ever* (Volume 2; ISACA Journal, p. 10). <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-2/why-cyber-insurance-needs-probabilistic-and-statistical-cyberrisk-assessments-more-than-ever>
- Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 40(1), 131–158. <https://doi.org/10.1057/gpp.2014.19>
- Blunt, R. (2021, January 29). The SolarWinds Cyberattack. *Senate RPC*. <https://www.rpc.senate.gov/policy-papers/the-solarwinds-cyberattack>
- Booth, P., Chadburn, R., Haberman, S., James, D., Khorasanee, Z., Plumb, R. H., & Rickayzen, B. (2020). *Modern actuarial theory and practice*. CRC Press.
- Cantrell, S. (2022, June 17). Systematic Reviews: 4. Search the Evidence. Retrieved July 7, 2022, from <https://guides.mclibrary.duke.edu/sysreview/search>
- Cebula, J. J., & Young, L. R. (2010). 'A Taxonomy of Operational Cyber Security Risks', Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.
- CISA. (2019). *Assessment of the Cyber Insurance Market*. [https://www.cisa.gov/sites/default/files/publications/19\\_1115\\_cisa\\_OCE-Cyber-Insurance-Market-Assessment.pdf](https://www.cisa.gov/sites/default/files/publications/19_1115_cisa_OCE-Cyber-Insurance-Market-Assessment.pdf)
- Cole, C., & Fier, S. (2021). An Empirical Analysis of Insurer Participation in the U.S. Cyber Insurance Market. *North American Actuarial Journal*, 25(2), 232–254. <https://doi.org/10.1080/10920277.2020.1733615>
- Computer Security Resource Center [CSRC]. (2022). *Cyber risk*. NIST. [https://csrc.nist.gov/glossary/term/cyber\\_risk](https://csrc.nist.gov/glossary/term/cyber_risk)
- Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. *BMC medical research methodology*, 11, 100. <https://doi.org/10.1186/1471-2288-11-100>
- Daykin, C. D., Pentikainen, T., & Pesonen, M. (1993). *Practical risk theory for actuaries*. Chapman and Hall/CRC.
- Department of Health. (2018). *Investigation: WannaCry cyber attack and the NHS - National Audit Office (NAO) Report* (SESSION 2017–2019). National Audit Office. <https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/>
- Dou, W., Tang, W., Wu, X., Qi, L., Xu, X., Zhang, X., & Hu, C. (2020). An insurance theory based optimal cyber-insurance contract against moral hazard. *Information Sciences*, 527, 576–589. <https://doi.org/10.1016/j.ins.2018.12.051>
- Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management & Insurance Review*, 24(1), 93–125. <https://doi.org/10.1111/rmir.12169>
- Eling, M., & Schnell, W. (2016). *Ten Key Questions on Cyber Risk and Cyber Risk Insurance* (p. 88). The Geneva Association. [https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf\\_public/cyber-risk-10\\_key\\_questions.pdf](https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber-risk-10_key_questions.pdf)



- FBI. (2018). *RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS*. Federal Bureau of Investigation. <https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections>
- Federal Trade Commission [FTC]. (2017, September 25). *The Equifax Data Breach*. Federal Trade Commission. <http://www.ftc.gov/equifax-data-breach>
- Fujs, D., Mihelic, A., Vrhovec, S., & Assoc Comp Machinery. (2019). *The power of interpretation: Qualitative methods in cybersecurity research* (WOS:000552726400092). <https://doi.org/10.1145/3339252.3341479>
- Green, J., & Thorogood, N. (2018). *Qualitative methods for health research*. Sage.
- IBM Cloud Education. (2020, July 15). *What is Machine Learning?* IBM. <https://www.ibm.com/cloud/learn/machine-learning>
- Innerhofer-Oberperfler, F., & Breu, R. (2010). Potential Rating Indicators for Cyberinsurance: An Exploratory Qualitative Study. In T. Moore, D. Pym, & C. Ioannidis (Eds.), *Economics of Information Security and Privacy* (pp. 249–278). Springer US. [https://doi.org/10.1007/978-1-4419-6967-5\\_13](https://doi.org/10.1007/978-1-4419-6967-5_13)
- Jarrow, R. A. (2008). Operational risk. *Journal of Banking & Finance*, 32(5), 870–879. <https://doi.org/10.1016/j.jbankfin.2007.06.006>
- Kenneally, E., Randazzese, L., & Balenson, D. (2018). Cyber Risk Economics Capability Gaps Research Strategy. *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–6. <https://doi.org/10.1109/CyberSA.2018.8551399>
- Keskin, O. F., Caramancion, K. M., Tatar, I., Raza, O., & Tatar, U. (2021). Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports. *Electronics*, 10(10), 1168. <https://doi.org/10.3390/electronics10101168>
- Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, 24, 35–61. <https://doi.org/10.1016/j.cosrev.2017.01.001>
- Marotta, A., & McShane, M. (2018). Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach. *Risk Management and Insurance Review*, 21(3), 435–452. <https://doi.org/10.1111/rmir.12109>
- McShane, M., & Nguyen, T. (2020). Time-varying effects of cyberattacks on firm value. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 45(4), 580–615. <https://doi.org/10.1057/s41288-020-00170-x>
- Moore, S. (2022, April 13). 7 Top Trends in Cybersecurity for 2022. *Gartner*. <https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022>
- Morgan, S. (2020, November 10). Cybercrime To Cost The World \$10.5 Trillion Annually By 2025. *Cybercrime Magazine*. <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>
- OECD. (2017). *Supporting an Effective Cyber Insurance Market—OECD Report for the G7 Presidency* (p. 20). <https://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf>
- Office of Cybersecurity, Energy Security, and Emergency Response. (2021). *Colonial Pipeline Cyber Incident*. Energy.Gov. <https://www.energy.gov/ceser/colonial-pipeline-cyber-incident>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W.,



- Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, n71. <https://doi.org/10.1136/bmj.n71>
- Rudden, J. (2022, January 11). *Global cyber insurance market size 2026*. Statista. <https://www.statista.com/statistics/1190800/forecast-cyber-insurance-market-size/>
- SAS. (2022). Statistical Analysis. [https://www.sas.com/en\\_us/insights/analytics/statistical-analysis.html](https://www.sas.com/en_us/insights/analytics/statistical-analysis.html)
- Schopf, J. (2010). *Towards a Prague Definition of Grey Literature*. <https://doi.org/10.71858>
- Shannon, R. E. (1975). *Systems Simulation: the Art and Science*. Englewood Cliffs: Prentice Hall.
- Smith, Z. M., Lostri, E., & Lewis, J. A. (2020). *The Hidden Costs of Cybercrime* (p. 38). McAfee.
- Tatar, U., Nussbaum, B., Gokce, Y., & Keskin, O. F. (2021). Digital force majeure: The Mondelez case, insurance, and the (un)certainly of attribution in cyberattacks. *Business Horizons*. <https://doi.org/10.1016/j.bushor.2021.07.013>
- Tondel, I., Seehusen, F., Gjaere, E., & Moe, M. (2016). *Differentiating Cyber Risk of Insurance Customers: The Insurance Company Perspective* (F. Buccafurri, A. Holzinger, P. Kieseberg, A. Tjoa, & E. Weippl, Eds.; WOS:000389019800012; Vol. 9817, pp. 175–190). [https://doi.org/10.1007/978-3-319-45507-5\\_12](https://doi.org/10.1007/978-3-319-45507-5_12)
- Value Momentum, (2022, January 15). 5 Ways to Drive Value with Insurance Data Analytics. <https://www.valuemomentum.com/blog/data-analytics-insurance/>
- Verlaine, M. (2021). On the extraction of cyber risks from structured products. *Applied Economics*. <https://doi.org/10.1080/00036846.2021.1998327>
- Wang, S. S. (1997). Aggregation of correlated Risk Portfolios: Models and Algorithms. Preprint Casualty Actuarial Society (CAS, 848–939).
- Yang, Y., Yang, Q., Yang, Z., & Xue, S. (2019b). Optimal Model Design for the Cyber-Insurance Contract with Asymmetric Information. *2019 International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 513–518. <https://doi.org/10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00104>
- Yang, Z., Liu, Y., Campbell, M., Ten, C.-W., Rho, Y., Wang, L., & Wei, W. (2020). Premium Calculation for Insurance Businesses Based on Cyber Risks in IP-Based Power Substations. *IEEE Access*, 8, 78890–78900. <https://doi.org/10.1109/ACCESS.2020.2988548>
- Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology? —A Systematic Review. *PLOS ONE*, 11(10), e0163477. <https://doi.org/10.1371/journal.pone.0163477>

## About The Society of Actuaries Research Institute

Serving as the research arm of the Society of Actuaries (SOA), the SOA Research Institute provides objective, data-driven research bringing together tried and true practices and future-focused approaches to address societal challenges and your business needs. The Institute provides trusted knowledge, extensive experience and new technologies to help effectively identify, predict and manage risks.

Representing the thousands of actuaries who help conduct critical research, the SOA Research Institute provides clarity and solutions on risks and societal challenges. The Institute connects actuaries, academics, employers, the insurance industry, regulators, research partners, foundations and research institutions, sponsors and non-governmental organizations, building an effective network which provides support, knowledge and expertise regarding the management of risk to benefit the industry and the public.

Managed by experienced actuaries and research experts from a broad range of industries, the SOA Research Institute creates, funds, develops and distributes research to elevate actuaries as leaders in measuring and managing risk. These efforts include studies, essay collections, webcasts, research papers, survey reports, and original research on topics impacting society.

Harnessing its peer-reviewed research, leading-edge technologies, new data tools and innovative practices, the Institute seeks to understand the underlying causes of risk and the possible outcomes. The Institute develops objective research spanning a variety of topics with its [strategic research programs](#): aging and retirement; actuarial innovation and technology; mortality and longevity; diversity, equity and inclusion; health care cost trends; and catastrophe and climate risk. The Institute has a large volume of [topical research available](#), including an expanding collection of international and market-specific research, experience studies, models and timely research.

Society of Actuaries Research Institute  
475 N. Martingale Road, Suite 600  
Schaumburg, Illinois 60173  
[www.SOA.org](http://www.SOA.org)