Mini Project - The Relationship Between Cyber Insurance and Supply Chain Security: A Systematic Review of Best Practices and Challenges

Table of Contents

[Publications 4](#_Toc149813255)

[Abstract 5](#_Toc149813256)

[Introduction 6](#_Toc149813257)

[Problem Statement 6](#_Toc149813258)

[Purpose and Objective 7](#_Toc149813259)

[Research questions 7](#_Toc149813260)

[Contributions of the Survey 8](#_Toc149813261)

[Related Work 9](#_Toc149813262)

[Methodology 10](#_Toc149813263)

[Ethical Considerations 13](#_Toc149813264)

[Significance and Impact 14](#_Toc149813265)

[The Evolution of Cyber Supply Chain Security 15](#_Toc149813266)

[Defining Cyber Supply Chain Security 15](#_Toc149813267)

[The Traditional Supply Chain: A Brief History 16](#_Toc149813268)

[The Digital Transformation of Supply Chains 17](#_Toc149813269)

[The Emergence of Cyber Supply Chain Security 17](#_Toc149813270)

[Cyber Supply Chain Security in Different Industries 18](#_Toc149813271)

[Current Trends and Challenges in Cyber Supply Chain Security 19](#_Toc149813272)

[Cyber Insurance Landscape in Supply Chain Security 20](#_Toc149813273)

[Overview of the Cyber Insurance Market 21](#_Toc149813274)

[Understanding Coverage and Pricing Models 22](#_Toc149813275)

[Types of Cyber Insurance Policies Relevant to Supply Chain Security 23](#_Toc149813276)

[Challenges in Implementing Cyber Insurance for Supply Chain Security 23](#_Toc149813277)

[The Role of Cyber Insurance in Supply Chain Security 24](#_Toc149813278)

[Unique Challenges of Implementing Cyber Insurance in the Context of Supply Chain Security 25](#_Toc149813279)

[Case Studies of Challenges Faced 26](#_Toc149813280)

[Assessment of Current Mitigation Strategies 27](#_Toc149813281)

[Best Practices in Leveraging Cyber Insurance for Supply Chain Cyber Resilience 28](#_Toc149813282)

[Review of Best Practices 28](#_Toc149813283)

[Best Practices in Selecting Cyber Insurance Policies for Supply Chain Security 30](#_Toc149813284)

[Role of Regulatory Bodies and Policies in Promoting Best Practices 31](#_Toc149813285)

[Potential Pitfalls and Recommendations 32](#_Toc149813286)

[Discussion 33](#_Toc149813287)

[Synthesis of Findings 34](#_Toc149813288)

[Cyber Insurance and Supply Chain Security: A Theoretical Perspective 35](#_Toc149813289)

[Practical Implications of Cyber Insurance for Supply Chain Security 37](#_Toc149813290)

[Contributions to Theory and Practice 39](#_Toc149813291)

[Limitations of the Study 41](#_Toc149813292)

[Final Thoughts and Conclusion 42](#_Toc149813293)

[References 45](#_Toc149813294)

# Publications

This Mini thesis has produced the following publications:

* ‘The Relationship Between Cyber Insurance and Supply Chain: A Review of Best Practices and Challenges,’ CSUR-2023-0639, ACM Computing Surveys (Under Review)

Authors: XXX, YYYY

* ‘Cyber Insurance as a Risk Mitigation Strategy in Digital Supply Chains’, 20th ANZAM Operations, Supply Chain and Services Management Symposium – 2023

Authors: XXX, YYY, ZZZ

# Abstract

This paper comprehensively examines the intersection of cyber insurance and supply chain security, exploring the role, benefits, challenges, and best practices of leveraging cyber insurance as an effective tool for managing and enhancing supply chain security. With the backdrop of an escalating frequency of sophisticated cyberattacks and the increasing interdependence of global supply chains, the importance of cyber insurance in mitigating cyber risks has never been more evident. Through an exhaustive analysis of the existing literature, the study provides a broad and deep perspective on the growing cyber insurance market, its correlation with supply chain security, and its unique challenges and benefits. The study further explores the intricacies of coverage and pricing models, contributing to an understanding of the multidimensional nature of cyber insurance. The research also probes into the role of regulatory bodies and policies in setting the standards for cyber insurance and discusses the practical implications of Australian law in this context. It sheds light on the effectiveness of current strategies to overcome challenges. It draws on real-world case studies to elucidate the role and impact of cyber insurance in managing supply chain cyber risks. This paper contributes to the existing body of knowledge in the field, providing practical insights for businesses, policymakers, and academia aiming to promote cyber resilience and effective risk management within supply chains. It acknowledges the limitations of the current research. It offers avenues for future research, emphasizing that the role of cyber insurance in securing supply chains is an ever-evolving, increasingly significant, and complex domain. The paper concludes that despite the present challenges, cyber insurance's potential to contribute to a robust and resilient supply chain is compelling and warrants continued research and policy development.

# 

# Introduction

In an interconnected digital landscape, businesses are increasingly vulnerable to cyber-attacks targeting supply chains, which are critical to global commerce (Deane et al., 2009; Ghadge et al., 2020a; Pandey et al., 2020). The 2017 Maersk cyber-attack, for instance, not only led to substantial losses but also illustrated the interconnectedness of supply chains and their far-reaching impact (Cyberattack: Maersk, 2017). This escalating risk landscape calls for innovative solutions like cyber insurance, a burgeoning financial safeguard against cyber-induced economic damages (Skeoch, 2022; Keegan, 2014). Existing literature insufficiently explores how cyber insurance can augment supply chain security, creating a knowledge gap (Linton et al., 2014a; Linton et al., 2014b). This review aims to elucidate this complex relationship, unearthing challenges and best practices involved in merging cyber insurance into supply chain risk management (Boyson, 2014a; Colicchia et al., 2019). By doing so, this study hopes to offer invaluable insights to stakeholders ranging from organizations to policymakers, ultimately promoting a more resilient digital supply chain (Cha, 2022; Cheung et al., 2021).

Subsequent sections will discuss key findings and implications, focusing on the practical and theoretical aspects of integrating cyber insurance into supply chain security. We aim to shed light on the multidisciplinary nature of this field, address legal considerations, and offer future research directions. This review highlights the pivotal role of cyber insurance in enhancing supply chain resilience and the necessity for a comprehensive framework to align insurance policies with supply chain vulnerabilities (Ghadge et al., 2020a; Boyson, 2014b; Bartol, 2014; Mishina et al., 2021; Creazza et al., 2022; Marotta et al., 2017; Romanosky et al., 2019). Through this analysis, the paper aims to contribute to ongoing efforts to strengthen cyber resilience in our interconnected world.

## Problem Statement

In our digitally connected world, supply chains are increasingly vulnerable to cyber-attacks, with ramifications echoing across entire networks and causing considerable financial and operational damage (Ghadge et al., 2020a; Deane et al., 2009; Pandey et al., 2020). Although cyber insurance has emerged as a key risk-mitigation strategy (Böhme & Schwartz, 2010; Skeoch, 2022), the existing research has not adequately explored its effective integration with supply chain security (Linton et al., 2014a; Cheung et al., 2021). Conventional economic models like the Gordon-Loeb model fall short of capturing the complexities in this space (Gordon & Loeb, 2002). Adding to the complexity, global supply chains are subject to a diverse regulatory landscape, varying by jurisdiction (Sokolov et al., 2014; Venter, 2014; Williams, 2014). This review aims to resolve these gaps and ambiguities by offering an in-depth look at current practices, challenges, and avenues for future research in cyber insurance and supply chain security. This investigation is critical due to the escalating cyber threats that jeopardize both global commerce and security (Al-Ansari & Alsubait, 2022).

## Purpose and Objective

This review explores the under-researched nexus between cyber insurance and supply chain security (Linton et al., 2014a). It aims to clarify cyber insurance's role in boosting supply chain resilience (Ghadge et al., 2020a; Skeoch, 2022) and to offer insights into integrating it into risk management strategies (Boyson, 2014a). The study will distill best practices for using cyber insurance against supply chain cyber risks (Deane et al., 2009). Using rigorous methodology (Bettany-Saltikov, 2010a), the review aspires to provide valuable guidance for stakeholders, such as organizations and policymakers, in enhancing cyber resilience through effective risk tools like cyber insurance.

## Research questions

The questions concentrate on three key themes:

* **Cyber Insurance Landscape in Supply Chain Security:** Building on Ghadge et al. (2020a) and Boyson (2014a), this question examines the variety of policies, their coverage scope, and pricing tailored to organizations in complex supply chains.
* **Implementation Challenges:** Inspired by Linton et al. (2014a) and Ghadge et al. (2020b), this question seeks to identify the specific hurdles in applying cyber insurance to supply chain security.
* **Best Practices:** Aligned with the works of Boyson (2014b) and Cheung et al. (2021), this question aims to spotlight effective strategies for employing cyber insurance to bolster supply chain resilience.

These questions intend to provide valuable insights into cyber insurance's role in supply chain security, thus enriching the growing field of study.

The research questions can be summarised as follows:

1. What is the current landscape of cyber insurance in the context of supply chain security, including the types of policies available, coverage, and pricing models tailored to the specific needs of organizations with complex supply chains?
2. What are the unique challenges faced by organizations and the cyber insurance industry in managing and insuring against supply chain cyber risks?
3. What are the best practices for leveraging cyber insurance to enhance supply chain cyber resilience?

Answering these research questions is expected to provide significant insights into the cyber insurance landscape for supply chain security, thereby contributing to the body of knowledge in this emerging field.

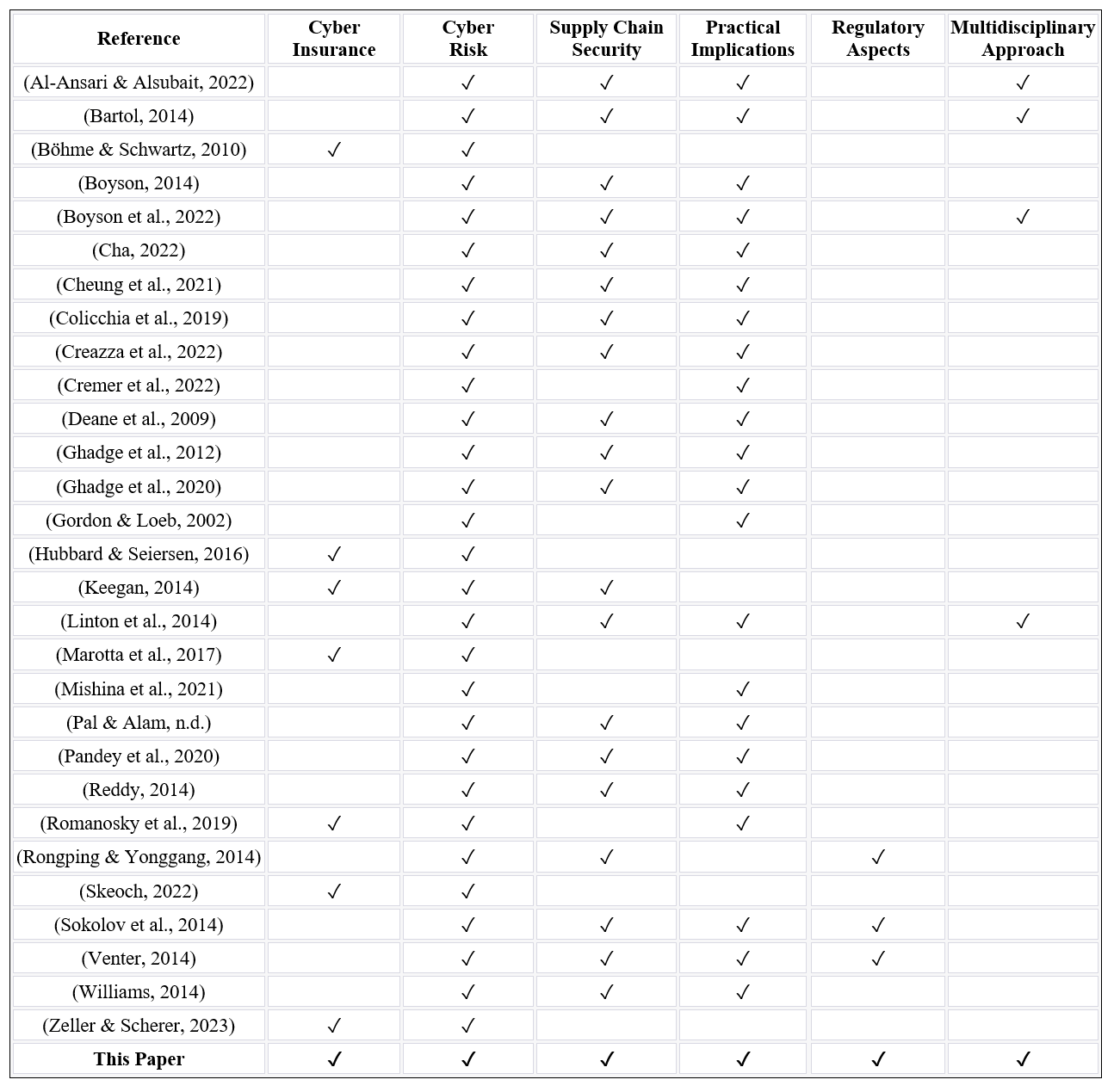
## Contributions of the Survey

This review fills a crucial gap in the literature on cyber insurance's role in supply chain security—a hitherto underexplored area. It adopts a multidisciplinary approach, combining insights from supply chain management, cyber risk, and insurance economics for a comprehensive view. The study delves into the current cyber insurance market, highlighting key players, market shares, and growth trends. Unique to this research is its focus on supply chain security within the cyber insurance realm. By unpacking challenges and potential solutions, it offers actionable risk management strategies. The study also explores Australian legal and regulatory contexts, providing a holistic understanding of implementing cyber insurance. The review is relevant to both academia and industry, offering theoretical insights and real-world applications. It also outlines avenues for future research, underlining its ongoing relevance to this critical area of study.

## Related Work

Existing studies delve into cyber risk, cyber insurance, or supply chain security, but none tackle the unique overlap that this paper investigates. Our research stands out for several reasons. First, it offers a holistic view, melding theoretical concepts with real-world applications in the context of supply chain cyber security. This includes a framework of best practices not thoroughly covered in earlier works. Second, while most referenced articles focus on isolated aspects like risk assessment or market dynamics, this research offers a comprehensive examination that stitches these themes together. It also adds a rarely discussed legal dimension, particularly focusing on Australian law.

Third, this study employs a multidisciplinary approach. Unlike prior work that may focus on one area, we draw insights from supply chain management, insurance economics, cyber risk, and legal studies for a rounded analysis. This multidisciplinary focus enables actionable, collaborative strategies for managing supply chain cyber risks. This systematic review uniquely fills several gaps: it offers a holistic, multidisciplinary exploration of cyber insurance in supply chain security, analyzes practical case studies, and incorporates overlooked legal and regulatory considerations. The table below shows the papers used in this literature review and groups them into their focus areas.



# Methodology

This systematic review will be guided by the well-regarded principles and practices set out by Bettany-Saltikov (2010a; 2010b). These guidelines have been chosen due to their stringent structure, providing a rigorous framework that ensures an in-depth and objective exploration of the subject at hand. For a thorough understanding of the interplay between cyber insurance and supply chain security, the study will adopt a mixed methods approach, merging both qualitative and quantitative research techniques.

Using the quantitative method, the study aims to pinpoint overarching trends and discernible patterns in the data, employing statistical tools to extract findings that can be generalized. Conversely, the research questions also mandate an in-depth exploration, a goal achieved through qualitative research. As underscored by scholars like Colicchia, Creazza, & Menachof (2019) and Creazza, Colicchia, Spiezia, & Dallari (2022), qualitative techniques play a pivotal role in unearthing the intricate layers of cybersecurity in supply chain contexts. In this vein, a meticulous thematic analysis will be employed on the chosen literature. Such an analysis will involve extracting, evaluating, and presenting patterns or themes present within the data. This thematic scrutiny will be both inductive—drawing insights straight from the data, and deductive—shaped by the study's guiding questions (Bettany-Saltikov, 2010b).

The rationale behind adopting a mixed methods approach hinges on the intricate and layered dynamics of cyber insurance's role in supply chain security. The qualitative facet lends depth and intricacy to the understanding, while the quantitative element broadens the study's horizon, capturing wider trends in the extant literature. By merging these techniques, the study aspires to provide a balanced, robust, and comprehensive perspective, recognizing the need for both extensive and intensive analyses to truly grasp the nexus between cyber insurance and supply chain security.

The systematic review has followed a 7-stage process, as described below:

A diagram of a stage

Description automatically generated with medium confidence

The table further details this process:

A close-up of a document

Description automatically generated with low confidence In conducting this systematic review, we employed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) flow model. PRISMA is a widely accepted standard for reporting in systematic reviews, ensuring transparency, consistency, and comprehensiveness in selecting and reporting studies. The PRISMA flow model enabled me to systematically sift through and select relevant studies, clearly visualizing the entire review process, from initial search to final inclusion. By adopting this approach, we aimed to enhance the robustness and replicability of this review. The PRISMA Flow model is shown below:

A screenshot of a computer

Description automatically generated

## Ethical Considerations

Despite the absence of direct human-subject interaction, ethical concerns are integral to this systematic review. Key ethical aspects include:

* Fair Representation of Sources: It is vital to accurately depict the original concepts, findings, and arguments from the cited literature (Bettany-Saltikov, 2010a). Misrepresenting or oversimplifying these can erode the review's credibility.
* Plagiarism: Proper citation is crucial to avoid plagiarism. Even paraphrased content must be duly cited to credit the original authors (Bettany-Saltikov, 2010a).
* Data Confidentiality: Discussing cyber insurance and supply chain security could involve sensitive data (Ghadge et al., 2020a). Responsible handling of this information, ensuring confidentiality and data security, is imperative (Keegan, 2014).
* Conflict of Interest: Any potential conflicts influencing the review should be transparently disclosed (Pal & Alam., 2017), fostering trust and maintaining the research's integrity.

By following these ethical guidelines, the review aims to maintain academic integrity, honor the contributions of other researchers, and responsibly contribute to the dialogue on cyber insurance and supply chain security.

## Significance and Impact

The rise of digital transformation and globalized supply chains has heightened businesses' vulnerability to cyber threats (Cheung et al., 2021; Bartol, 2014). Due to the interconnectedness of supply chains, cyber-attacks now have multi-entity, far-reaching implications (Boyson, 2014a; Ghadge et al., 2020a). In this context, cyber insurance is gaining prominence as an essential risk mitigation tool (Skeoch, 2022). Though vital, the role of cyber insurance in supply chain security is relatively unexplored in academia (Linton et al., 2014a). This review aims to address this gap, offering insights into current practices, challenges, and opportunities for implementing cyber insurance in supply chain risk management (Creazza et al., 2022; Deane et al., 2009). The findings will benefit diverse stakeholders—businesses, insurers, policymakers, and scholars—by offering a holistic view of how cyber insurance can fortify supply chain resilience.

This research also sets the groundwork for my future PhD project, aiming to develop a quantitative risk model for critical infrastructures relevant to cyber insurance. Through analyzing existing challenges and practices, this review will offer crucial parameters for the model's construction. Also, by utilizing rigorous methodology (Bettany-Saltikov, 2010a), the review enriches academic discourse and offers practical insights for crafting resilient digital business strategies.

The societal impact is also notable, offering both academic and real-world applications. The review serves as a blueprint for enhancing cyber resilience in a rapidly evolving threat landscape. It aims, alongside my future PhD research, to equip society with knowledge and tools to better defend against escalating cyber threats.

# The Evolution of Cyber Supply Chain Security

The rise of digital transformation has driven industries to optimize supply chain operations while also necessitating enhanced cyber protections. This chapter outlines the evolution of cyber supply chain security, emphasizing its role in safeguarding interconnected digital systems within supply chains. Al-Ansari and Alsubait (2022) underscore machine learning's role in threat prediction, while Bartol (2014) advocates a multidisciplinary approach, marking cybersecurity as integral to traditional supply chain methods. Digital transformation significantly impacts supply chains. Keegan (2014) discusses this from an insurance perspective, highlighting the importance of cybersecurity. Emerging technologies like IoT, AI, and blockchain have reshaped supply chain practices but also introduced new risks (Deane et al., 2022). Boyson et al. (2022) stress the need for proactive cyber risk management as a strategic focus. Industry-specific approaches are also vital; Cheung et al. (2021) emphasize this in the context of logistics, while Creazza et al. (2022) explore the challenges of incorporating cybersecurity during digital transformation. Noteworthy case studies, like the Maersk Global Supply Chain Meltdown, offer real-world lessons, emphasizing the need for strong security measures. The literature collectively contributes to our understanding of the evolution of cyber supply chain security. They highlight the integration of cybersecurity into traditional supply chain practices, the impact of digital transformation on supply chains, the emergence of cyber supply chain security as a distinct field, and the challenges faced in different industries. These insights form the foundation for comprehending the current trends and challenges in cyber supply chain security.

## Defining Cyber Supply Chain Security

Cyber supply chain security aims to shield supply chain information systems from threats. Al-Ansari and Alsubait (2022) advocate for machine learning to foresee and counter cyber threats, aligning with a proactive, tech-enabled risk strategy. Bartol (2014), on the other hand, calls for a multidisciplinary angle, integrating cybersecurity within traditional supply chain management for a rounded risk view. This security understanding isn't limited to single organizations but requires collective efforts. Boyson et al. (2022) further highlight the importance of inter-organizational information sharing for enhanced resilience. They assert that isolated security measures aren't enough; collaboration across the supply chain is essential. Keegan (2014) introduces cyber insurance as a supplementary risk management tool, aiding loss recovery. Cyber supply chain security is an evolving, multi-layered concept. It entails proactive vulnerability detection, technological utilization, cross-disciplinary and collaborative tactics, and adaptation to digital shifts. This adaptive outlook spans multiple dimensions, including predictive analytics, third-party risks, and incident response. As such, it informs future dialogues and equips organizations to develop robust, flexible strategies to mitigate cyber threats.

## The Traditional Supply Chain: A Brief History

Traditionally, supply chain management focussed on physical logistics like storage and delivery. Bartol (2014) advocates for a multidisciplinary approach, stressing that cybersecurity should blend with traditional supply chain practices. This melding of disciplines like IT, risk management, and operations lets organizations form holistic strategies against cyber risks and signals the evolving nature of supply chain management. Boyson (2014) highlights how strategic control over critical IT has been revolutionized, acknowledging that traditional supply chain models have adapted to meet cyber threats. Organizations are increasingly recognizing and addressing these vulnerabilities to improve security. Moreover, Deane et al. (2022) also point out the transformative role of emerging technologies like IoT and AI on supply chains. While these technologies enhance connectivity and automation, they also bring new cyber risks, necessitating an adaptive approach to traditional practices. Cheung et al. (2021), on the other hand, explore the sector-specific challenges in cybersecurity, suggesting that the cybersecurity strategies need to be customized to the unique needs of sectors like retail or healthcare.

The digitalization of traditional supply chains offers both advantages and introduces cybersecurity risks. The literature underscores the necessity of embedding cybersecurity into established practices, advocating for sector-specific solutions. This historical context equips organizations to better address the challenges posed by cyber threats in contemporary supply chains.

## The Digital Transformation of Supply Chains

Digital transformation has significantly altered supply chains through the advent of technologies like IoT, AI, and blockchain, reshaping global operations. Keegan (2014) from the insurance industry emphasizes the increasing importance of cybersecurity within this transformation, noting how insurance can financially safeguard against cyber threats. As outlined by Deane et al. (2022), IoT enhances connectivity and data exchange, AI boosts analytics and automation, and blockchain provides secure, decentralized data storage. These technologies offer improved efficiency and transparency but also introduce vulnerabilities. Mishina et al. (2021) spotlight the emerging "silent" cyber risks within digital supply chains, warning that digital interconnections create avenues for cyberattacks. The literature broadly agrees on the need for a comprehensive cybersecurity approach. Pal & Alam (2017) stress the necessity of robust risk management, including regular assessments and incident response plans. Protective measures should encompass secure network architectures, encryption, and continuous monitoring.

While digital transformation offers efficiency and visibility, it also introduces cybersecurity challenges that need proactive management. Organizations should embed cybersecurity into their digital supply chains through risk assessments, robust protective measures, and fostering a culture of cybersecurity awareness to ensure resilience and security.

## The Emergence of Cyber Supply Chain Security

The growing complexity of digital supply chains has necessitated a specialized area of focus—cyber supply chain security. Initially overlooked, this field has evolved to become essential in the business realm. Factors like escalating cyber threats, technology integration, and reliance on third-party vendors amplify its importance, although it remains a challenging task to secure increasingly global, interconnected supply chains. Boyson et al. (2022) shed light on the necessity for proactive cyber risk management in digital supply chains, endorsing the view that the field is evolving to meet ever-changing threats and secure digital assets. Similarly, Creazza et al. (2022) note a rising awareness among supply chain managers about the significance of managing cyber risks, underscoring the need for resilience and operational continuity.

For effective security, Bartol (2014) also argues for a multidisciplinary approach involving supply chain partners, IT experts, and cybersecurity professionals. Cross-disciplinary collaboration is crucial in crafting comprehensive risk management strategies. Furthermore, Colicchia et al. (2019) point out that industry-specific challenges necessitate tailored cybersecurity measures to counter unique vulnerabilities in sectors like retail, manufacturing, and healthcare.

In essence, the burgeoning field of cyber supply chain security is driven by an evolving threat landscape, technology integration, and a recognized need for specialized security. A collaborative, industry-specific approach is vital for implementing effective security measures, which in turn enhances the resilience and continuity of digital supply chains.

## Cyber Supply Chain Security in Different Industries

Cyber supply chain security is a multi-industry concern requiring specialized strategies for each sector. Cheung et al. (2021) stress the distinct challenges each industry faces, underscoring the need for sector-focused cyber risk solutions. In healthcare, Pal & Alam (2017) emphasize protecting patient data and medical device integrity, requiring strict controls and compliance with data protection laws.

In retail, Ghatge et al. (2020) point to risks involving e-commerce and payment systems. They suggest measures like strong encryption protocols and secure payment gateways to maintain customer trust, which is critical for financial and reputational stability. In manufacturing, Boyson (2014) also highlights the need to protect intellectual property and secure control systems. Strategies often involve robust access controls, anomaly detection, and backup mechanisms to prevent disruptions, production delays, or loss of intellectual property.

Although industries have unique cyber supply chain concerns, foundational cybersecurity practices are universal. These include secure networking, patch management, access controls, and employee training. Moreover, inter-industry collaboration is crucial for mitigating cyber risks effectively. Keegan (2014) also notes how the insurance industry encourages robust cybersecurity measures by offering insurance coverage against cyber threats, playing a key role in setting guidelines and standards.

## Current Trends and Challenges in Cyber Supply Chain Security

Understanding the ever-changing realm of cyber supply chain security is vital for both practitioners and researchers. Current literature points to a growing interconnectedness of supply chains through cloud computing, IoT, and AI, creating new vulnerabilities (Deane et al., 2022). Adapting to these changes by weaving cybersecurity into supply chain processes is essential (Bartol, 2014). A shift towards proactive cyber risk management is another key trend. Organizations are moving from mere reactive stances to identifying risks and implementing preventive measures (Creazza et al., 2022). This proactive strategy aligns with a broader industry focus on risk management and resilience against evolving threats.

The intricate web of supply chain connections compounds the security challenges. A breach in one entity can reverberate through the entire chain (Boyson et al., 2022). The global nature of supply chains, involving multiple partners across regions, heightens these challenges (Pandey et al., 2020). Case studies like the Maersk Global Supply Chain Meltdown serve as cautionary examples of the severe fallout from cyber incidents. Pandey et al. (2020) and Cremer et al. (2022) add further insights into cyber risk assessment. While Pandey et al. propose a framework for risk assessment in global chains, Cremer et al. highlight the hurdles in data availability for effective risk analysis. The lack of comprehensive data is a recurrent issue, necessitating better data sharing and standardized reporting.

Keeping pace with the ever-evolving cyber threats is another obstacle. Continuous monitoring and the implementation of adaptive security measures are critical (Keegan, 2014). Emerging technologies like AI and machine learning are increasingly utilized for threat detection (Al-Ansari & Alsubait, 2022). Organizational culture and employee training are often underemphasized but vital aspects of cybersecurity (Cheung et al., 2021). A well-rounded strategy should not only include technical defenses but also address the complexities of supply chains and compliance with growing regulations.

The field of cyber supply chain security is in a continuous state of evolution, requiring a multifaceted and agile approach. By acknowledging these trends and challenges, organizations can better secure their supply chains against an increasingly complex threat landscape.

# Cyber Insurance Landscape in Supply Chain Security

The nexus of cybersecurity and supply chain management has introduced considerable challenges. One key strategy to address these challenges is the incorporation of cyber insurance. This topic has seen growing attention as a valuable tool for managing cyber risks in complex supply chains, as elaborated by authors like Böhme and Schwartz (2010) and Marotta et al. (2017). These works stress the need to fully grasp cyber insurance policies and their relevance to supply chain security, emphasizing the concept's utility in broader risk management strategies.

Understanding the objectives of cyber insurance is pivotal. Al-Ansari and Alsubait (2022) discuss the use of machine learning to anticipate cyber threats, underlining the proactive aspects of cyber insurance. This enables companies to use predictive analytics for identifying vulnerabilities and implementing preventive actions, thus aligning with their risk management goals. Cyber insurance also plays a vital role in fostering supply chain resilience. Sector-specific approaches to managing cyber risks are essential, as pointed out by Cheung et al. (2021). Cyber insurance contributes to resilience by offering financial safeguards and support during cyber incidents, enhancing its value as a risk mitigation tool.

The literature suggests a varied adoption and understanding of cyber insurance across sectors and organizations. While some works focus on technical elements like risk modeling (Al-Ansari and Alsubait, 2022; Böhme and Schwartz, 2010), others advocate for tailored, industry-specific approaches (Cheung et al., 2021). These variations reflect the complexities and diversity of challenges in supply chain security. Moreover, Marotta et al. (2017) illuminate the evolving array of policy options, stressing the importance for organizations to stay updated and select appropriate coverage.

This section offers a snapshot of cyber insurance's role, objectives, and changing landscape in the realm of supply chain security. By embracing this concept, organizations can incorporate it into their overarching risk management plans. The chapter aims to critically analyze the present state of cyber insurance in this domain, setting the stage for subsequent discussions on its implementation challenges and best practices for enhancing cyber resilience in supply chains.

## Overview of the Cyber Insurance Market

The cyber insurance sector is rapidly expanding due to increasing cyber-attacks and heightened awareness of digital risks, especially within supply chains. Unlike traditional insurance markets with abundant historical data, cyber insurance is an evolving field still in its maturation phase. This chapter explores policy types, coverage, and pricing models relevant to supply chain security.

As digital transformation gains pace, cyber insurance becomes not only a financial safeguard but also a marker of an organization's cyber risk management commitment. Various authors, such as Cremer et al. (2022), have noted this growing market fueled by the desire of companies to mitigate cyber risks effectively. Companies are increasingly requiring not just their own cyber insurance but also mandating it for their vendors, which is crucial for reinforcing supply chain security. The market has its challenges, as outlined by Mishina et al. (2021), including 'silent cyber risks' or cyber-related losses not explicitly covered or excluded in policies. These dynamic risks necessitate a careful evaluation of policy terms to ensure sufficient supply chain coverage.

Moreover, the market is leaning towards more dynamic pricing models, as pointed out by Skeoch (2022), with the extension of the Gordon-Loeb model to cyber insurance. This reflects efforts to align pricing with the ever-changing risk landscape. Additional factors affecting coverage and pricing include the integration of cybersecurity measures into existing supply chain practices, as emphasized by Bartol (2014) and Reddy (2014).

The cyber insurance market is an essential component of cyber supply chain security. Its growth, coupled with emerging challenges and trends, indicates ongoing efforts to refine pricing and offer innovative coverage options. Effective use of this evolving tool depends on accurate risk pricing, policy alignment with current threats, and a wide understanding across industries. Organizations can use this knowledge to inform their cyber insurance decisions, ensuring effective risk management in their supply chains.

## Understanding Coverage and Pricing Models

Understanding the types of risks a business aims to offset is crucial for shaping cyber insurance policy coverage. Rongping and Yonggang (2014) stress the need to comprehend the policy's scope, detailing first-party coverage for breach responses and third-party coverage for legal liabilities. This knowledge allows organizations to align policies with their risk management goals.

Pricing is another vital aspect of cyber insurance. Hubbard and Seiersen (2016) note that the cost depends on multiple variables, such as industry, size, past incidents, and cybersecurity protocols. Understanding these metrics helps companies gauge premium fairness and make informed investment decisions. Factors like company characteristics and cybersecurity measures also affect pricing and coverage, as per Lai et al. (2017). Strong cybersecurity and risk management practices often translate into wider coverage and more favorable premiums, whereas poor practices or a history of incidents can lead to higher costs or restricted options.

Tailored coverage that matches an organization’s specific risk profile is essential. Key considerations like industry type, size, and cybersecurity health influence both coverage scope and pricing. Proactive risk management practices can secure more comprehensive coverage at competitive rates. Continuous evaluation of these factors, especially considering evolving cyber threats, is imperative for maintaining effective coverage while optimizing investment.

## Types of Cyber Insurance Policies Relevant to Supply Chain Security

Cyber insurance has evolved to meet the diverse risks across various industries. Marotta et al. (2017) categorize policies into first-party and third-party coverages. First-party typically covers expenses like forensic investigations and business interruptions due to data breaches. Third-party focuses on liabilities arising from such breaches, including legal costs and settlements. These distinctions help organizations tailor their coverage needs, particularly in the context of supply chain security.

The types of coverage extend beyond first and third-party, as outlined by Marotta et al. (2017). They include cyber extortion coverage, safeguarding against ransomware costs, and cyber-physical damages coverage, protecting against physical harm caused by cyber events. In supply chain security, third-party coverage gains prominence, offering a safety net against the widespread impacts of a cyber event.

Moreover, Bartol (2014) stresses the need for policy evaluation based on the unique needs of supply chain operations. Policy relevance varies; manufacturers may prioritize first-party coverage for operational disruptions, while data-centric logistics providers could find third-party coverage equally critical. Sector-specific considerations, such as patient data in healthcare or supply chain disruptions in manufacturing, further guide policy selection.

Organizations must align their insurance policy types with their specific vulnerabilities and risk appetite within supply chains. This requires a thorough evaluation of the coverage types offered and an understanding of industry-specific risks (Bartol, 2014; Marotta et al., 2017).

# Challenges in Implementing Cyber Insurance for Supply Chain Security

As organizations increasingly digitize, the complexity of their supply chain security grows. The advent of cyber insurance offers a financial safety net against cyber threats, yet its integration into supply chain security is not without challenges. This section explores these hurdles to help organizations make informed decisions in adopting cyber insurance as part of their broader cybersecurity strategy. The growing relevance of cyber insurance in supply chain security is underscored by authors like Ghadge et al. (2020a) and Boyson (2014a). These works affirm its value as a proactive risk management tool, emphasizing the need to grasp its nuances specifically related to supply chains. Further research by authors such as Linton et al. (2014a) and Ghadge et al. (2020b) explores the complexities in the application of cyber insurance to supply chain security. Key challenges include the fluid nature of supply chains, the web of stakeholder interconnections, and the difficulty in precisely measuring cyber risks. This highlights the need for custom strategies when embedding cyber insurance into supply chain security. Understanding these challenges is pivotal for fortifying supply chain resilience. By analyzing the various studies, we can offer a nuanced view of both the value and the difficulties involved in incorporating cyber insurance into supply chain security plans. This serves as a foundation for addressing specific challenges in future discussions.

## The Role of Cyber Insurance in Supply Chain Security

Cyber insurance serves as a financial cushion for organizations facing cyber threats, covering expenses like data breach investigations, regulatory fines, and business disruptions. Its significance is amplified in the intricate networks of supply chains, where a security lapse at any point can have a cascading impact. In this context, cyber insurance manages systemic risk by offering coverage for incidents at various nodes of the supply chain. Ghadge et al. (2020a) underscore the financial safeguarding role of cyber insurance, pointing out its ability to offload financial risks from organizations to insurers. This enables efficient resource allocation and quicker recovery post-incident, contributing to the resilience and sustainability of supply chains. Boyson (2014a) similarly highlights how cyber insurance assists organizations in mitigating financial impacts, specifically by covering costs like incident response and business interruptions. The insurance thus becomes a vital enabler for business continuity within supply chains.

Keegan (2014) further discusses cyber insurance as a motivator for better cybersecurity practices. Insurers often offer premium discounts to policyholders who implement effective risk management, encouraging investments in cybersecurity and strengthening the supply chain’s overall security posture. Cheung et al. (2021) also accentuate the need for customized cyber insurance solutions to suit the unique risks and vulnerabilities across different sectors in the supply chain, thereby making it a more nuanced risk management tool.

The reviewed literature underscores cyber insurance’s multifaceted role in enhancing supply chain security. It not only provides financial relief and fosters quicker recovery but also incentivizes improved cybersecurity measures and offers tailored solutions for sector-specific challenges. Therefore, cyber insurance serves as a critical tool for bolstering the resilience and security of supply chains in an evolving cyber threat landscape.

## Unique Challenges of Implementing Cyber Insurance in the Context of Supply Chain Security

Cyber insurance offers promise in managing cyber risks within supply chains, yet its implementation comes with its own set of hurdles. Linton et al. (2014a) and Ghadge et al. (2020b) point out that the ever-changing and multi-layered nature of supply chains complicates the accurate assessment of cyber risks. These supply chains involve a plethora of interconnected players like suppliers, manufacturers, and customers, each having their own cybersecurity protocols and risk profiles. This complexity, along with regular changes in technologies and partnerships, further muddles the risk evaluation and insurance process.

Mishina et al. (2021) spotlight another hurdle: the intricate web of shared risks due to the interconnectedness of supply chain entities. A cyber incident in one organization can cascade into system-wide disruptions, making it difficult to assign responsibility, allocate liabilities, and determine appropriate coverage. This necessitates a collective approach to risk management involving information sharing and close cooperation among all stakeholders.

In addition, Bartol (2014) emphasizes the absence of standard frameworks for cyber risk evaluation in supply chains as a significant obstacle. The lack of consistency in risk assessment methodologies makes it challenging for insurers to set precise premiums. Furthermore, limited historical data specific to supply chain cyber risks hampers accurate risk quantification, setting it apart from traditional insurance types, which rely on abundant historical data for pricing.

Boyson et al. (2022), on the other hand, draw attention to the evolving cyber threat landscape, requiring insurers to continually revise their coverage options and risk strategies. Keeping up-to-date with emerging threats such as ransomware and supply chain attacks calls for ongoing research, as well as collaborations with cybersecurity experts.

To navigate these challenges—be it the dynamic nature of supply chains, intertwined stakeholder risks, lack of standardized risk metrics, or the fast-paced evolution of cyber threats—both insurers and organizations must engage in joint efforts. This includes creating robust risk assessment models, fostering data sharing, and designing flexible insurance solutions. Recognizing and tackling these issues is crucial for effective risk management and the overall resilience of supply chains. It's also a prerequisite for making well-informed decisions concerning cyber insurance investments, setting the stage for the subsequent chapter focusing on best practices to mitigate these challenges.

## Case Studies of Challenges Faced

Exploring case studies provides key insights into the intricate issues and repercussions of cyber incidents in supply chains. These studies serve as practical illustrations of challenges that organizations face when incorporating cyber insurance into supply chain security. For example, the Maersk Global Supply Chain Meltdown showcases the sweeping effects of a cyberattack on a leading shipping company. This study amplifies the difficulty in gauging and addressing cyber risks in intricate supply chains, stressing the need for thorough risk assessments and apt insurance coverage.

Contrastingly, studies like those by Mishina et al. (2021) and Boyson et al. (2022) explore industry-specific challenges. Mishina et al. (2021) delve into a cyberattack on a healthcare supply chain, illuminating unique vulnerabilities and regulatory hurdles in the healthcare sector. The case underlines the imperative for sector-specific insurance policies that cater to healthcare’s unique risk profile, including data sensitivity and compliance mandates.

Boyson et al. (2022), on the other hand, focus on a cyberattack impacting a defense contractor. This case zeroes in on challenges prevalent in sectors that are both highly regulated and security-sensitive. It accentuates the complexities of crafting insurance coverage compliant with strict regulations while also ensuring supply chain resilience and robust incident response.

These cases collectively identify recurring hurdles such as limited understanding of insurance options, challenges in loss estimation, and the necessity for integrated cybersecurity across supply chains. Additionally, they advocate for proactive incident response, employee training, and consistent cybersecurity audits. These case-based lessons underscore the importance of investing in comprehensive cybersecurity, understanding insurance options deeply, and ongoing risk evaluation. Such insights can guide the formulation of dynamic risk management strategies, insurer collaboration, and the implementation of all-encompassing security measures, thereby bolstering supply chain resilience against cyber threats.

## Assessment of Current Mitigation Strategies

As organizations confront distinct challenges in integrating cyber insurance into supply chain security, various countermeasures have surfaced. Prominent among these is the adoption of risk management frameworks. Cremer et al. (2022) advocate for a structured, proactive approach to identifying, assessing, and managing cyber risks. By weaving cyber insurance into these frameworks, organizations can harmonize their risk-reducing tactics with their insurance provisions, offering a holistic approach to secure supply chains.

Another focal point is cyber hygiene, emphasized by Pandey et al. (2020). Key practices such as software updates, patch management, employee education, and network monitoring help in curtailing cyber risks. Merging risk management frameworks with cyber hygiene forms a potent strategy. While frameworks help in risk identification and evaluation, cyber hygiene contributes to preventive measures, building a layered defense against both internal and external threats.

The efficacy of these mitigation measures depends on multiple variables, like organizational culture, resource allocation, and the fluid nature of cyber risks. Customization to align with an organization’s unique supply chain, industry norms, and risk tolerance is vital. Periodic assessments and audits are essential for fine-tuning these strategies. Partnering with insurance providers is equally crucial; they can offer specialized guidance and coverage options that resonate with an organization’s specific risks and countermeasures. This collaboration enriches an organization's perspective on emerging trends and best practices in supply chain security. Continual evaluation and adaptation of these strategies are indispensable to cope with the ever-changing cyber risk landscape and to fortify supply chain resilience.

# Best Practices in Leveraging Cyber Insurance for Supply Chain Cyber Resilience

As tech integration in supply chain processes deepens, the imperative for robust cybersecurity measures grows. Cyber insurance is increasingly recognized as a critical component for managing cyber risks in supply chain operations. This section delves into best practices for harnessing cyber insurance to bolster supply chain resilience. Notable studies like Ghadge et al. (2020a) stress the need for best practices in risk management, incident response, and business continuity within the realm of cyber insurance. They argue that these actions are pivotal for elevating supply chain security and resilience. Likewise, Boyson (2014b) underscores the value of best practices in fortifying overall supply chain resilience, citing the supportive role of cyber insurance.

The literature consistently points to the indispensability of best practices in achieving cyber resilience in supply chains. These studies suggest that cyber insurance should not act in isolation but be part of a larger risk management framework involving key practices like risk assessment, incident response coordination, and collaboration. Further insights from Marotta et al. (2017) emphasize the importance of selecting suitable insurance policies tailored for supply chain security, reinforcing the need for best practices in policy selection and adaptation. These collective perspectives underscore that while cyber insurance isn't a cure-all, it remains a vital element in a comprehensive approach to cyber risk management.

## Review of Best Practices

Effective practices for utilizing cyber insurance in securing supply chains are proven methods yielding positive results in mitigating cyber threats. As interconnected supply chains become more vulnerable, cyber insurance is increasingly vital for maintaining resilience against such risks. This section synthesizes best practices informed by key authors in the field.

The survey of these practices reveals their diverse role in bolstering supply chain cyber resilience. A recurring theme is proactive risk management. Ghadge et al. (2020a) stress the need for consistent risk assessments to spot vulnerabilities and target security initiatives. They also underscore the value of organized incident response plans for efficient recovery from cyber events. These practices are foundational for supply chain resilience. Beyond risk management, strong security infrastructure is crucial, as highlighted by Boyson (2014b), who recommends advanced cybersecurity tools like intrusion detection, firewalls, and encryption as vital defenses against cyber threats.

Another critical practice pinpointed is thorough incident response planning. Mishina et al. (2021) advocate for clearly defined response procedures, periodic drills, and streamlined communication channels. Collaboration among supply chain actors is another key element; sharing threat intelligence strengthens collective cyber defense. Industry collaboration, public-private partnerships, and active participation in cybersecurity forums enable effective information exchange and provide early warnings against emerging threats (Boyson, 2014b). Employee training and awareness, emphasized by Mishina et al. (2021), are also essential. Cultivating cybersecurity awareness equips staff to be vigilant contributors to supply chain security.

In the realm of interconnected supply chains, these practices take on heightened importance. A single cyber event can trigger a cascade, affecting multiple entities. Thus, resilience requires not only individual organizations but also their network partners to adopt these best practices. While specific practices may differ based on each organization’s unique risks, the core principle remains constant: the creation of supply chains that are both resilient and well-defended against cyber threats.

## Best Practices in Selecting Cyber Insurance Policies for Supply Chain Security

The rising frequency and severity of cyber threats amplify the role of cyber insurance in safeguarding supply chains. Mitigating financial risks from such incidents, cyber insurance boosts supply chain resilience. However, selecting the right policy involves understanding an organization's risk profile and comparing different coverage options. The literature outlines key practices for choosing tailored cyber insurance policies. A pivotal practice is a detailed vulnerability assessment of the supply chain. Marotta et al. (2017) stress the need to identify key assets, analyze threats, and evaluate the impact of cyber incidents. This groundwork helps organizations focus on the risks to be addressed via insurance.

Another important step is matching policy coverage with identified risks. Firms should scrutinize various insurance offerings to ensure they meet specific supply chain risks. Mishina et al. (2021) suggest aligning policies with identified threats, taking into account factors like data breach and business interruption coverages, third-party liability, and legal expenses. The financial strength and reputation of insurance providers also merit consideration. Boyson et al. (2022) point out the value of insurers with a strong track record in claims handling and incident support. Open dialogue with insurers is essential to tailor the policy to an organization's specific vulnerabilities and needs. Moreover, it's vital to understand policy limitations or exclusions and how they fit within an organization’s risk tolerance.

Maintaining transparent communication with insurers is key. This helps insurers comprehend an organization’s risk landscape, enabling them to offer customized coverage. Additionally, insurance should integrate seamlessly with existing risk management approaches, supplementing other security initiatives like response plans and employee training. Other factors like waiting periods, sub-limits, and event-specific restrictions should also be scrutinized.

Best practices can differ based on an organization's characteristics and industry. Tailoring cyber insurance strategies to individual needs is essential, as is ongoing evaluation to adapt to evolving cyber threats. By adhering to these optimal practices, organizations can choose policies that not only provide robust coverage but also align with their risk profiles, enhancing supply chain security.

## Role of Regulatory Bodies and Policies in Promoting Best Practices

In the context of cyber supply chain security and insurance, regulators and policymakers are crucial in setting standards and promoting best practices. Regulatory interventions can both improve cybersecurity measures and encourage companies to integrate cyber insurance into their risk management. Active engagement with regulatory bodies is essential, as Romanosky et al. (2019) suggest. This involvement helps companies comprehend the regulatory environment, contribute to policy discussions, and align their cyber insurance practices with industry norms. Being up-to-date on regulatory shifts is vital due to the evolving nature of cyber threats. Mishina et al. (2021) underscore the importance of regularly tracking changes in regulations and accordingly adjusting cyber insurance plans. This requires following updates from regulatory agencies, participating in industry groups, and consulting experts for compliance guidance.

Regulatory alignment is also critical. Regulations often set minimum cybersecurity requirements and may necessitate specific insurance coverage. Bartol (2014) advises organizations to assess their insurance policies in relation to these regulations for sufficient coverage. Incentives like reduced premiums may also be offered to organizations adopting effective cyber risk management, as mentioned by Romanosky et al. (2019). In Australia, key frameworks like the Privacy Act 1988 and the Notifiable Data Breaches (NDB) scheme directly influence cyber insurance practices. The Privacy Act, which includes the Australian Privacy Principles (APPs), governs how organizations handle personal data and sets the standard for data breach management. Compliance with this Act is crucial for customer trust and legal obligations. The NDB scheme, initiated in 2018, mandates that organizations notify both affected individuals and the Office of the Australian Information Commissioner (OAIC) about significant data breaches. Cyber insurance can help manage the financial and reputational risks associated with these breaches, aligning with the scheme's focus on transparency and accountability.

In addition to general laws, industry-specific guidelines also exist. The Australian Cyber Security Centre (ACSC) provides sector-specific resources, such as the Essential Eight strategies for cybersecurity. Adherence to these guidelines can enhance cyber resilience and ensure regulatory compliance. Financial institutions, in particular, should heed regulations from the Australian Prudential Regulation Authority (APRA), like Prudential Standard CPS 234, which focuses on information security. Given the dynamic regulatory landscape, staying informed about changes in laws and standards is essential for organizations. Active engagement and ongoing monitoring allow companies to adapt their cyber insurance approaches in line with evolving regulatory expectations.

## Potential Pitfalls and Recommendations

Navigating best practices in the realm of cyber insurance for enhancing supply chain resilience poses certain challenges. Recognizing and proactively addressing these pitfalls can optimize cyber insurance benefits and ensure robust risk mitigation. One common challenge is the insufficient risk assessment, as emphasized by Mishina et al. (2021). Incomplete assessments can result in underestimating the required coverage or selecting ill-suited policies. Therefore, organizations should allocate appropriate resources to perform comprehensive risk assessments that tailor insurance coverage to their specific risk profile.

Limited comprehension of insurance terms is another pitfall highlighted by Boyson et al. (2022). The complexity of policy terms can lead to misunderstandings about coverage scope. To mitigate this, it's advisable to consult with cybersecurity and insurance experts for policy interpretation, ensuring clear awareness of potential coverage limitations or exclusions. Complexity also affects the policy selection process, making it difficult to compare offerings. To overcome this, organizations should engage in thorough due diligence, reviewing factors like coverage scope, limits, and deductibles. Insurance brokers can offer invaluable insights into navigating policy complexities.

To navigate these challenges, enhancing internal cybersecurity capabilities is essential. Investment in cybersecurity training, adoption of industry best practices, and vigilance about emerging threats can align insurance needs effectively. Furthermore, periodic reassessment of coverage is crucial to adapt to the evolving risk landscape. Effective collaboration between cybersecurity, risk management, and insurance teams is also vital. Open communication facilitates the identification of emerging threats and the development of risk mitigation strategies. This collaborative approach can amplify the organization's cyber resilience. Lastly, it's beneficial to liaise with industry-specific regulatory bodies and laws, like the Security of Critical Infrastructure Act 2018 or the Privacy Act 1988 in Australia, for compliance guidance. Adherence to such regulations can provide a roadmap for cybersecurity and insurance requirements.

While cyber insurance is a key asset in managing supply chain cyber risks, its effective implementation demands careful planning, open communication, and continuous management. When properly employed, cyber insurance can substantially bolster supply chain cyber resilience.

# Discussion

This section synthesizes key findings and insights on the intersection of cyber insurance and supply chain security. Authors like Ghadge et al. (2020a) and Boyson (2014b) underscore cyber insurance's role as a risk management instrument that bolsters supply chain resilience. These insights affirm that cyber insurance is pivotal in reducing cyber risks and aiding recovery after a cyber event. The collation of these findings enables a comprehensive grasp of the research landscape. Through critical analysis, we identify recurring themes, major recommendations, and overarching conclusions, presenting a unified summary that highlights the thesis' contributions. This discussion further delves into the theoretical aspects of cyber insurance's role in supply chain security, informed by works like Ghadge et al. and Boyson. This theoretical grounding offers a lens for evaluating the practical impacts of cyber insurance. On the practical front, analysis of works such as Marotta et al. (2017) and Cremer et al. (2022) allows us to explore the real-world implications of cyber insurance within supply chain security. Revisiting our research objectives and evaluating findings against them confirms the extent of the study's success. This approach also reveals gaps in current knowledge that can inform future research directions in the domain of cyber insurance and supply chain security.

## Synthesis of Findings

In synthesizing the findings of previous chapters, the overarching narrative indicates a significant shift towards cyber supply chain security, prompted by technological advancement and the digitalization of supply chains. The synthesis of findings reveals several recurring themes and recommendations. One prominent theme is the recognition of cyber insurance as a valuable risk management tool for organizations operating within complex supply chains. Ghadge et al. (2020a) and Boyson (2014b) emphasize the importance of cyber insurance in mitigating financial losses and facilitating recovery in the event of a cyber incident. Marotta et al. (2017) contribute to this theme by providing insights into the different policy types and coverage areas relevant to supply chain security. This synthesis underscores the consensus among the articles regarding the positive role of cyber insurance in enhancing supply chain resilience.

Another significant theme that emerges is the need for a comprehensive and multidisciplinary approach to supply chain security. Bartol (2014) discusses the integration of cybersecurity practices into supply chain management, emphasizing the importance of collaboration among different departments and stakeholders. This theme is reinforced by articles such as Creazza et al. (2022) and Pandey et al. (2020), which highlight the importance of proactive risk assessment, incident response planning, and regular policy review. The synthesis underscores the holistic nature of supply chain security, which requires the involvement of various disciplines to effectively address cyber risks. The synthesis also reveals the role of regulatory bodies and policies in promoting best practices in cyber insurance and supply chain security. Romanosky et al. (2019) discuss the potential benefits of regulatory intervention, such as the establishment of cybersecurity standards and incentives for adopting cyber insurance. This finding highlights the importance of regulatory frameworks in driving the adoption of best practices and ensuring a consistent and secure supply chain environment.

While there is agreement on the value of cyber insurance in supply chain security, there may be variations in the specific recommendations and approaches proposed by different authors. These variations can be attributed to factors such as the industry context, organizational size, and geographic location. However, the synthesis of findings indicates that despite these variations, the overall message is consistent: Cyber insurance plays a crucial role in mitigating cyber risks and enhancing supply chain resilience.

## Cyber Insurance and Supply Chain Security: A Theoretical Perspective

Theoretical perspectives offer conceptual frameworks for understanding the dynamics and implications of cyber insurance in the context of supply chain security. Ghadge et al. (2020a) provide insights into the theoretical concept of risk management, highlighting how cyber insurance can be viewed as a risk mitigation tool. They emphasize the role of cyber insurance in transferring and managing financial risks associated with cyber incidents, thereby enhancing supply chain security. This theoretical perspective aligns with broader risk management theories, emphasizing identifying, assessing, and mitigating risks to ensure organizational resilience. Risk management theory forms a foundational premise for the relevance of cyber insurance. Traditional risk management strategies often include risk avoidance, risk reduction, risk sharing, and risk retention. In this context, cyber insurance becomes a key tool for risk sharing. As companies grapple with the exponential growth in cyber threats and their potential impacts on supply chains, the ability to share and transfer some of this risk to insurance providers can be a strategic move, enabling organizations to manage financial volatility associated with potential cyber incidents. In contrast, Boyson (2014b) introduces the theoretical lens of resilience to understand the relationship between cyber insurance and supply chain security. Resilience theory recognizes that organizations should not solely focus on preventing cyber incidents but also on their ability to recover and adapt in the face of disruptions. From this perspective, cyber insurance can be seen as a mechanism supporting supply chain resilience by providing financial resources and assistance during recovery. This theoretical perspective emphasizes the importance of integrating insurance into broader resilience strategies to enhance supply chain security.

Challenges also arise when we consider the application of principal-agent theory. The principal (insured company) and agent (insurer) relationship is riddled with issues of asymmetric information and moral hazard. Asymmetric information, where the insurer has less information about the actual cyber risk profile compared to the insured, can lead to adverse selection. Moral hazard occurs post-insurance acquisition, where the insured company may have less incentive to invest in other cybersecurity measures. These inherent challenges influence the effectiveness of cyber insurance as a tool for enhancing supply chain security. The resource-based view (RBV) provides another theoretical lens to understand the role of cyber insurance. From this perspective, cyber insurance can be seen as a 'resource' or 'capability' that a firm can leverage to gain a competitive advantage. However, the extent to which it contributes to sustained competitive advantage is contingent upon how it is managed in conjunction with other resources and capabilities within the firm. Cyber insurance should be seen as a part of a comprehensive cyber risk management strategy rather than an end-all solution.

The theoretical perspectives on cyber insurance in supply chain security are multifaceted. Some articles may emphasize risk management theories, focusing on the financial aspects of cyber insurance and the role of risk assessment and mitigation. Others may adopt a broader perspective, incorporating resilience theories and recognizing the interconnectedness of supply chain security with organizational resilience. While the articles offer different theoretical perspectives, they collectively highlight the value proposition of cyber insurance in enhancing supply chain security. The theoretical frameworks provide a conceptual understanding of the mechanisms through which cyber insurance contributes to supply chain resilience, risk management, and continuity. It is important to acknowledge that the theoretical perspectives presented in the articles may vary based on the authors' backgrounds, research objectives, and the specific context of supply chain security. Further research and exploration of additional theoretical frameworks may be necessary to provide a more comprehensive understanding of the theoretical underpinnings of cyber insurance in supply chain security. In synthesizing these theoretical perspectives, it becomes clear that the value proposition of cyber insurance for supply chain security is complex. These theories provide conceptual foundations for understanding the role and impact of cyber insurance in mitigating risks, enhancing resilience, and ensuring the continuity of supply chains. Its usefulness is undeniable, given the escalating cyber risk landscape. However, it also introduces new challenges that must be carefully navigated for optimal results. Balancing the benefits and challenges requires a nuanced understanding of the theoretical underpinnings and practical implications, which will be further discussed in the following sections.

## Practical Implications of Cyber Insurance for Supply Chain Security

Moving from the theoretical to the practical, the implications of cyber insurance for supply chain security are significant. Building upon our earlier discussions, this section delves into how these implications manifest in real-world scenarios. Practical implications of cyber insurance in supply chain security revolve around the considerations, challenges, and benefits associated with its implementation. Marotta et al. (2017) provide insights into practical considerations when selecting cyber insurance policies. They emphasize the importance of conducting thorough risk assessments, aligning coverage with identified risks, and engaging in effective communication with insurers. These practical considerations highlight the need for a comprehensive understanding of an organization’s supply chain and cyber risks to make informed decisions regarding cyber insurance.

Moreover, there is the direct financial benefit that cyber insurance provides in the event of a cyber incident. Costs associated with data breaches, ransomware attacks, and other cyber events can be immense, as evidenced by numerous case studies, including that of the healthcare provider discussed. These costs can range from direct expenses, such as paying ransom or recovery specialists, to indirect costs, such as business interruption, reputational damage, and potential lawsuits. Cyber insurance, in these instances, provides a safety net, covering a range of these expenses and mitigating the financial impact on the organization. However, the value proposition of cyber insurance extends beyond this direct financial benefit. Insurance providers often require or encourage insured parties to maintain a certain level of cybersecurity standards, leading to improved security postures. This proactive risk management can significantly contribute to strengthening supply chain security.

Despite these benefits, the practical implementation of cyber insurance isn't without its challenges. The principal-agent issues discussed earlier have direct practical implications. Insured companies might face high premiums if insurers perceive them to be high-risk due to asymmetric information. Moreover, companies might become complacent in their cybersecurity efforts post-insurance acquisition, exacerbating the moral hazard problem. Moreover, as scholars like Biener et al. (Article 8) and Bolot and Lelarge (Article 14) pointed out, the cyber insurance market lacks standardized policy definitions and terms. This lack of standardization can create confusion and potentially lead to gaps in coverage that only become apparent when a cyber incident occurs.

In the context of supply chain security, another critical challenge emerges - the complexity of managing risk across multiple entities. A cyber-incident at one supply chain partner can have a cascading effect, impacting multiple parties. Traditional cyber insurance policies may not adequately cover these complex, inter-organizational cyber risks, creating a gap in the company's risk management strategy. Furthermore, Cremer et al. (2022) shed light on the challenges and benefits of implementing cyber insurance in supply chain security. The challenges include the dynamic nature of supply chains, the difficulty in accurately assessing cyber risks across the supply chain, and the complexity of policy terms and conditions. These challenges underscore the need for effective risk management strategies, collaboration among stakeholders, and clear communication with insurers. On the other hand, the benefits of cyber insurance include financial protection against cyber incidents, assistance in the recovery process, and access to expertise and resources offered by insurance providers.

Additionally, articles such as Bartol (2014) highlight the importance of integrating cyber insurance with established supply chain practices. This integration requires a multidisciplinary approach involving stakeholders from IT, operations, legal, and risk management departments. Practical implications of cyber insurance in supply chain security include the need for collaboration among these departments to ensure that insurance coverage aligns with the unique cyber risks and vulnerabilities associated with supply chain operations. Effective utilization of cyber insurance in supply chain security also requires continuous evaluation and adjustment of coverage. Mishina et al. (2021) discuss the importance of regular policy reviews and updates to ensure that the coverage remains relevant and responsive to evolving cyber threats. Organizations need to stay informed about emerging risks, technological advancements, and changes in their supply chain operations to adapt their insurance coverage accordingly. Moreover, practical implications include the establishment of robust risk management frameworks and incident response plans. Articles such as Boyson et al. (2022) emphasize the importance of proactive risk management practices, including conducting vulnerability assessments, implementing cybersecurity measures, and developing incident response capabilities. Cyber insurance can complement these practices by providing financial resources and expertise to support organizations in their response and recovery efforts.

It is important to note that the practical implications may vary depending on organizational factors, the industry sector, and the specific context of supply chain operations. Different industries may have unique cyber risks and regulatory requirements that need to be considered when implementing cyber insurance for supply chain security. The practical implications of cyber insurance in supply chain security are multifaceted and complex, encompassing careful consideration of specific supply chain risks, selection of appropriate policies, collaboration among stakeholders, continuous evaluation and adjustment of coverage, and the establishment of robust risk management frameworks and incident response plans. Organizations can leverage cyber insurance as a strategic tool to enhance their overall cyber resilience, mitigate financial losses associated with cyber incidents, and effectively respond to and recover from cyber threats. While cyber insurance can be a powerful tool for financial risk transfer and incentivizing better security practices, it also brings new challenges and complexities that businesses must navigate carefully. The value of cyber insurance, therefore, largely depends on how effectively it's integrated into a broader, comprehensive cyber risk management strategy.

## Contributions to Theory and Practice

This study makes considerable contributions to both theory and practice in the realm of cyber insurance in supply chain security. By bridging the gap between theory and practice, the study provides a comprehensive and practical framework for understanding and leveraging cyber insurance for enhanced supply chain security. In terms of theory, the research contributes to the understanding of risk management in supply chain security. Authors such as Ghadge et al. (2020a) emphasize the role of cyber insurance as a risk mitigation tool, enabling organizations to transfer and manage cyber risks within their supply chains. By examining the relationship between cyber insurance and risk management, the study provides insights into the theoretical foundations of cyber risk assessment, risk transfer, and risk mitigation strategies. These findings advance the theoretical knowledge by highlighting the importance of cyber insurance in addressing the complex and evolving risks in supply chain operations. Furthermore, the research contributes to the theoretical understanding of resilience in the context of supply chain security. Resilience refers to an organization’s ability to adapt and recover from disruptions, including cyber incidents. By exploring the role of cyber insurance in enhancing supply chain resilience, the study extends the theoretical framework of resilience in the context of cyber risks. It highlights how cyber insurance can act as a protective measure, enabling organizations to recover and resume operations in a timely manner. This contribution enhances our theoretical understanding of resilience, particularly in the specific context of supply chain security.

From a theoretical perspective, this research synthesizes findings from various articles, extending our understanding of cyber insurance in a supply chain context. It provides a comprehensive view of the current cyber insurance landscape and its influence on supply chain security, which has been fragmented in the existing literature. Furthermore, the insights gained from the detailed analysis of current challenges and best practices provide a platform for future academic research. The study also enhances theoretical models on cyber risk management by integrating elements of cyber insurance.

From a practical perspective, the research offers valuable insights and recommendations for organizations seeking to leverage cyber insurance for supply chain security. The identification and analysis of best practices, as highlighted in articles like Marotta et al. (2017) and Cremer et al. (2022), provide practical guidance to organizations. These best practices include conducting thorough risk assessments, customizing coverage to align with identified risks, and integrating cyber insurance into existing risk management practices. By implementing these practices, organizations can enhance their supply chain security and effectively manage cyber risks. From a practical standpoint, this research offers actionable insights for businesses, insurance providers, and policy-makers. The detailed exploration of best practices, as well as potential pitfalls in leveraging cyber insurance for supply chain security, provides a roadmap for businesses in various industries. These insights can guide them in choosing suitable insurance policies, implementing effective risk management strategies, and enhancing overall supply chain cyber resilience. Case studies presented in the research, such as the ones from the Healthcare sector, can be seen as practical examples of how cyber insurance can mitigate the impacts of cyber threats.

## Limitations of the Study

In the interest of academic rigor, it is important to acknowledge the potential limitations of this research. Firstly, the limitations of the study can be attributed to the breadth and depth of the literature covered by the articles. While these articles provide a comprehensive overview of the topic, they may not encompass the entirety of the research conducted in the field. It is possible that some relevant studies were not included in the analysis, which could introduce a potential bias and limit the scope of the findings (Cremer et al., 2022; Marotta et al., 2017).

Additionally, the articles may vary in terms of their research methodologies, sample sizes, and geographic contexts. This variation can affect the generalizability and applicability of the findings to different organizational settings and industries (Ghadge et al., 2020a; Boyson, 2014b). The limited geographic coverage of the articles may restrict the generalizability of the findings to specific regions, and caution should be exercised when extrapolating the results to other contexts (Romanosky et al., 2019; Zeller and Scherer, 2023).

Another limitation to consider is the potential for publication bias in the articles. Published articles tend to report positive and significant results, while studies with null or negative findings may be underrepresented. This can introduce a bias towards certain research findings and limit the comprehensive understanding of the field (Hubbard and Seiersen, 2016; Reddy, 2014).

Furthermore, the limitations of the study also include the lack of primary data collection. The analysis and synthesis of existing articles can be constrained by the data availability and quality of the selected studies. While these sources provide a robust foundation, the reliance on published materials may introduce some bias, as the findings may reflect the perspectives or interests of the original authors. The reliance on secondary data sources may limit the depth of analysis and the ability to address specific research questions (Linton et al., 2014a; Ghadge et al., 2020b).

Lastly, the fast-paced evolution of cyber threats and the corresponding evolution of the cyber insurance market make it challenging to provide a fully up-to-date perspective. The research relies on the most recent data and insights available up to the point of the study, but the findings could be influenced by future developments. These recent developments and advancements may not be reflected in the analysis, potentially limiting the currency and relevance of the findings (Mishina et al., 2021; Boyson et al., 2022).

It is important to acknowledge these limitations to provide a balanced and transparent assessment of the study. Future research should aim to address these limitations by incorporating a wider range of literature, employing diverse research methodologies, and considering recent developments in the field. By addressing these limitations, researchers can further enhance the understanding of cyber insurance and supply chain security. Despite these limitations, the research strives to offer a comprehensive understanding of the role of cyber insurance in supply chain security. It presents a balanced perspective, taking into account various viewpoints from the literature and real-life case studies while also recognizing the areas that need further exploration. The limitations also provide opportunities for future research to delve deeper into specific areas and contribute further to this growing field of study.Top of Form

# Final Thoughts and Conclusion

This paper has provided a comprehensive exploration of the role of cyber insurance in supply chain security. The necessity of this exploration has been substantiated by a confluence of events in the digital landscape, primarily the escalating frequency and sophistication of cyberattacks, the growing interdependence of global supply chains, and the amplification of cyber risks due to these intertwined dynamics. The findings highlight the importance of cyber insurance as a risk management tool for organizations operating within complex supply chains (Ghadge et al., 2020a; Boyson, 2014b). By leveraging cyber insurance, organizations can mitigate financial losses, enhance their cyber resilience, and facilitate recovery in the event of a cyber incident (Marotta et al., 2017; Cremer et al., 2022).

The study's contributions to theory include an examination of key theoretical perspectives such as risk management, resilience, and the value proposition of cyber insurance in supply chain security (Ghadge et al., 2020a; Boyson, 2014b). By exploring these concepts, the thesis has enhanced our understanding of the underlying mechanisms and dynamics in the field. From a practical standpoint, the study has identified best practices in selecting cyber insurance policies, establishing frameworks for cyber supply chain security, and utilizing cyber insurance for risk mitigation and response (Marotta et al., 2017; Cremer et al., 2022). These insights guide organizations and insurance providers in developing effective strategies and policies and inform policymakers in their endeavors to regulate and shape this burgeoning market.

The implications for practice and policy are significant. The research underscores the need for collaboration among stakeholders, including government agencies, industry associations, insurers, and academia, to address supply chain cyber risks (Sokolov et al., 2014; Zeller and Scherer, 2023). The study also highlights the importance of regulatory frameworks, industry standards, and incentives to promote the adoption of cyber insurance and improve supply chain security (Romanosky et al., 2019; Hubbard and Seiersen, 2016).

The findings from the cross-examination of articles have facilitated a deep understanding of the cyber insurance market, its role in supply chain security, its challenges, best practices, and theoretical implications. Further, real-world instances reflected the tangible value of cyber insurance in mitigating the repercussions of a cyber incident in the supply chain. However, this thesis has not shied away from acknowledging the complexity and challenges that underpin cyber insurance, particularly in the context of supply chain security. From intricate risk assessment and pricing to legal and regulatory considerations, there is a clear indication that cyber insurance is not a panacea but a component of a more comprehensive cyber risk management strategy. It is essential to acknowledge the limitations of the study, which include potential biases in the selection of articles, constraints in the scope and methodology, and the dynamic nature of the field itself (Mishina et al., 2021; Boyson et al., 2022). These limitations provide opportunities for future research to further investigate and refine the understanding of cyber insurance in supply chain security.

Future research should focus on areas such as resilience assessment frameworks, behavioral and psychological factors, dynamic risk assessment methodologies, and cyber insurance education and awareness (Ghadge et al., 2020a; Marotta et al., 2017). Additionally, cross-disciplinary approaches integrating expertise from cybersecurity, risk management, insurance, and supply chain management can drive innovation and advance the field (Ghadge et al., 2020b; Creazza et al., 2022).

While this thesis has provided a snapshot of the current state of cyber insurance in supply chain security, the picture is ever evolving. The digitization trend is unabating, and with it, the sophistication of cyber threats continues to increase. Consequently, the role of cyber insurance in securing supply chains will continue to evolve and grow in significance and complexity. In conclusion, the interplay of cyber risk, supply chains, and insurance presents a fascinating area of study. While challenges abound, the potential of cyber insurance to contribute to robust and resilient supply chains is compelling. Future research, policy development, and industry practices should continue to innovate and refine our approach to using cyber insurance as a crucial instrument in our arsenal against the ever-present and growing specter of cyber threats.

# References

Al-Ansari, A. O., & Alsubait, T. M. (2022). Predicting Cyber Threats Using Machine Learning for Improving Cyber Supply Chain Security. *Proceedings of 2022 5th National Conference of Saudi Computers Colleges, NCCC 2022*, 123–130. https://doi.org/10.1109/NCCC57165.2022.10067692

Alberto Redondo, P., Torres-Barrán, A., Ríos Insua, D., & Domingo, J. (2019). *Assessing Supply Chain Cyber Risks*.

Bartol, N. (2014). Cyber supply chain security practices DNA – Filling in the puzzle using a diverse set of disciplines. *Technovation*, *34*(7), 354–361. https://doi.org/10.1016/J.TECHNOVATION.2014.01.005

Bettany-Saltikov, J. (2010a). Learning how to undertake a systematic review: part 1. *Nursing Standard (Royal College of Nursing (Great Britain) : 1987)*, *24*(50), 47–55. https://doi.org/10.7748/NS2010.08.24.50.47.C7939

Bettany-Saltikov, J. (2010b). Learning how to undertake a systematic review: Part 2. *Nursing Standard (Royal College of Nursing (Great Britain) : 1987)*, *24*(51). https://doi.org/10.7748/NS2010.08.24.51.47.C7943

Böhme, R., Laube, S., & Riek, M. (2019). A Fundamental Approach to Cyber Risk Analysis. *CASUALTY ACTUARIAL SOCIETY*, *0012,0002*, 161–18.

Böhme, R., & Schwartz, G. (2010). Modeling Cyber-Insurance: Towards A Unifying Framework. *Workshop on the Economics of Information Security (WEIS), Harvard, June 2010* .

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, *34*(7), 342–353. https://doi.org/10.1016/J.TECHNOVATION.2014.02.001

Boyson, S., Corsi, T. M., & Paraskevas, J. P. (2022). Defending digital supply chains: Evidence from a decade-long research program. *Technovation*, *118*. https://doi.org/10.1016/j.technovation.2021.102380

Cha, S. Y. (2022). The art of cyber security in the age of the digital supply chain: detecting and defending against vulnerabilities in your supply chain. *The Digital Supply Chain*, 215–233. https://doi.org/10.1016/B978-0-323-91614-1.00013-7

Cheung, K. F., Bell, M. G. H., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, *146*, 102217. https://doi.org/10.1016/J.TRE.2020.102217

Colicchia, C., Creazza, A., & Menachof, D. A. (2019). Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management*, *24*(2), 215–240. https://doi.org/10.1108/SCM-09-2017-0289

Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2022). Who cares? Supply chain managers’ perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management*, *27*(1), 30–53. https://doi.org/10.1108/SCM-02-2020-0073

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice 2022 47:3*, *47*(3), 698–736. https://doi.org/10.1057/S41288-022-00266-6

*Cyberattack: The Maersk Global Supply Chain Meltdown Case Solution And Analysis, HBR Case Study Solution & Analysis of Harvard Case Studies*. (2019). https://www.thecasesolutions.com/cyberattack-the-maersk-global-supply-chain-meltdown-178615

*Cyberattack: The Maersk Global Supply-Chain Meltdown*. (2019). https://store.hbr.org/product/cyberattack-the-maersk-global-supply-chain-meltdown/W19132

*Cyber-Attacks on Industrial Assets Cost Firms Millions - Jun 2, 2022*. (n.d.). Retrieved August 20, 2023, from https://newsroom.trendmicro.com/2022-06-02-Cyber-Attacks-on-Industrial-Assets-Cost-Firms-Millions

Deane, J. K., Ragsdale, C. T., Rakes, T. R., & Rees, L. P. (2009). Managing supply chain risk and disruption from IT security incidents. *Operations Management Research*, *2*(1), 4–12. https://doi.org/10.1007/S12063-009-0018-2

Eling, M., Nuessle, D., & Staubli, J. (2022). The impact of artificial intelligence along the insurance value chain and on the insurability of risks. *Geneva Papers on Risk and Insurance: Issues and Practice*, *47*(2), 205–241. https://doi.org/10.1057/S41288-020-00201-7/TABLES/8

Fan, Y., & Stevenson, M. (2018). A review of supply chain risk management: definition, theory, and research agenda. *International Journal of Physical Distribution and Logistics Management*, *48*(3), 205–230. https://doi.org/10.1108/IJPDLM-01-2017-0043/FULL/PDF

Gatzlaff, K. M., & McCullough, K. A. (2010). The Effect of Data Breaches on Shareholder Wealth. *Risk Management and Insurance Review*, *13*(1), 61–83. https://doi.org/10.1111/J.1540-6296.2010.01178.X

Ghadge, A., Dani, S., & Kalawsky, R. (2012). Supply chain risk management: Present and future scope. *The International Journal of Logistics Management*, *23*(3), 313–339. https://doi.org/10.1108/09574091211289200/FULL/XML

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management*, *25*(2), 223–240. https://doi.org/10.1108/SCM-10-2018-0357

*Global shipping feels fallout from Maersk cyber attack | Reuters*. (2017). https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19K2LE

Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457. https://doi.org/10.1145/581271.581274

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, *34*(5), 509–519. https://doi.org/10.1016/J.JACCPUBPOL.2015.05.001

Gurtu, A., & Johny, J. (2021). Supply Chain Risk Management: Literature Review. *Risks 2021, Vol. 9, Page 16*, *9*(1), 16. https://doi.org/10.3390/RISKS9010016

Herath Hermantha, & Herath Tejaswini. (2011). (PDF) Copula Based Actuarial Model for Pricing Cyber-Insurance Policies. *Insurance Markets and Companies 2(1)*. https://www.researchgate.net/publication/228280083\_Copula\_Based\_Actuarial\_Model\_for\_Pricing\_Cyber-Insurance\_Policies

Hubbard, D. W., & Seiersen, R. (2016). How to Measure Anything in Cybersecurity Risk. *How to Measure Anything in Cybersecurity Risk*. https://doi.org/10.1002/9781119162315

Ingram, D., & Bush, E. (2013). Collective Approaches to Risk in Business: An Introduction to Plural Rationality Theory. *North American Actuarial Journal*, *17*(4), 297–305. https://doi.org/10.1080/10920277.2013.847781

Keegan, C. (2014). Cyber security in the supply chain: A perspective from the insurance industry. *Technovation*, *34*(7), 380–381. https://doi.org/10.1016/J.TECHNOVATION.2014.02.002

Khan, O., & Burnes, B. (2007). Risk and supply chain management: Creating a research agenda. *The International Journal of Logistics Management*, *18*(2), 197–216. https://doi.org/10.1108/09574090710816931

Linton, J. D., Boyson, S., & Aje, J. (2014). The challenge of cyber supply chain security to research and practice – An introduction. *Technovation*, *34*(7), 339–341. https://doi.org/10.1016/J.TECHNOVATION.2014.05.001

Logue, K. D., & Shniderman, A. B. (2021). The Case for Banning (and Mandating) Ransomware Insurance. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3907373

Louis, M., & Pagell, M. (2019). Categorizing Supply Chain Risks: Review, Integrated Typology and Future Research. *Springer Series in Supply Chain Management*, *7*, 329–366. https://doi.org/10.1007/978-3-030-03813-7\_20/COVER

MacCarthy, B. L., Ahmed, W. A. H., & Demirel, G. (2022). Mapping the supply chain: Why, what and how? *International Journal of Production Economics*, *250*, 108688. https://doi.org/10.1016/J.IJPE.2022.108688

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

Mishina, R., Tanimoto, S., Goromaru, H., Sato, H., & Kanai, A. (2021). A Visualization Model for Silent Cyber Risks Contained in Emerging Risks. *2021 IEEE 10th Global Conference on Consumer Electronics, GCCE 2021*, 498–499. https://doi.org/10.1109/GCCE53005.2021.9621766

Monroe, R. W., Teets, J. M., & Martin, P. R. (2014). Supply chain risk management: An analysis of sources of risk and mitigation strategies. *International Journal of Applied Management Science*, *6*(1), 4–21. https://doi.org/10.1504/IJAMS.2014.059291

Pal, O., & Alam, B. (2017). Cyber Security Risks and Challenges in Supply Chain. *International Journal of Advanced Research in Computer Science*, *8*(5). www.ijarcs.info

Pal, R., Huang, Z., Lototsky, S., Yin, X., Liu, M., Crowcroft, J., Sastry, N., De, S., & Nag, B. (2021). Will Catastrophic Cyber-Risk Aggregation Thrive in the IoT Age? A Cautionary Economics Tale for (Re-)Insurers and Likes. *ACM Transactions on Management Information Systems*, *12*(2), 17. https://doi.org/10.1145/3446635

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103–128. https://doi.org/10.1108/JGOSS-05-2019-0042/FULL/PDF

Qazi, A., & Gaudenzi, B. (2016). Supply chain risk management: creating an agenda for future research. *International Journal of Supply Chain and Operations Resilience*, *2*(1), 12. https://doi.org/10.1504/IJSCOR.2016.075896

Qazi, A., Quigley, J., & Dickson, A. (2015). Supply Chain Risk Management: Systematic literature review and a conceptual framework for capturing interdependencies between risks. *IEOM 2015 - 5th International Conference on Industrial Engineering and Operations Management, Proceeding*. https://doi.org/10.1109/IEOM.2015.7093701

Reddy, D. (2014). Criticality analysis and the supply chain: Leveraging representational assurance. *Technovation*, *34*(7), 362–379. https://doi.org/10.1016/J.TECHNOVATION.2014.01.009

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

Rongping, M., & Yonggang, F. (2014). Security in the cyber supply chain: A Chinese perspective. *Technovation*, *34*(7), 385–386. https://doi.org/10.1016/J.TECHNOVATION.2014.02.004

Siciliano, G. G., & Gaudenzi, B. (2018). The role of supply chain resilience on IT and cyber disruptions. *Lecture Notes in Information Systems and Organisation*, *24*, 57–69. https://doi.org/10.1007/978-3-319-62636-9\_4

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

Sokolov, A., Mesropyan, V., & Chulok, A. (2014). Supply chain cyber security: A Russian outlook. *Technovation*, *34*(7), 389–391. https://doi.org/10.1016/J.TECHNOVATION.2014.01.004

Son, C. E., & Son, C. E. (2018). Supply Chain Risk Management: A Review of Thirteen Years of Research. *American Journal of Industrial and Business Management*, *8*(12), 2294–2320. https://doi.org/10.4236/AJIBM.2018.812154

*The Untold Story of NotPetya, the Most Devastating Cyberattack in History | WIRED*. (2018). https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Uuganbayar, G., Yautsiukhin, A., Martinelli, F., & Massacci, F. (2021). Optimisation of cyber insurance coverage with selection of cost effective security controls. *Computers & Security*, *101*, 102121. https://doi.org/10.1016/J.COSE.2020.102121

Venter, H. S. (2014). Security issues in the security cyber supply chain in South Africa. *Technovation*, *34*(7), 392–393. https://doi.org/10.1016/J.TECHNOVATION.2014.02.005

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/J.COSE.2013.04.004

Williams, C. (2014). Security in the cyber supply chain: Is it achievable in a complex, interconnected world? *Technovation*, *34*(7), 382–384. https://doi.org/10.1016/J.TECHNOVATION.2014.02.003

Zeller, G., & Scherer, M. (2023). Risk mitigation services in cyber insurance: optimal contract design and price structure. *Geneva Papers on Risk and Insurance: Issues and Practice*. https://doi.org/10.1057/S41288-023-00289-7