University of Piraeus
School of Information and Communication Technologies
Department of Digital Systems

Postgraduate Program of Studies
MSc Digital Systems Security

Master Thesis

Cyberinsurance as a Risk Management Tool

Supervisor Professor: S. Gritzalis

Kanavas Andreas a.kanavas@ssl-unipi.gr mte2011

Piraeus
24/09/2023

Summary

In summary, this thesis comprehensively examines the field of cyber insurance, its applications, advantages, and challenges, offering insights and guidelines for leveraging cyber insurance services in the modern cybersecurity landscape. This Thesis is divided into six main chapters:

Chapter 1 introduces the topic of cyber insurance and its significance in addressing cyber threats and risks within businesses and organizations. It outlines the objectives and structure of the paper.

Chapter 2 provides an in-depth exploration of cyber insurance, starting with its definition and a thorough analysis of cyber threats and risks in modern business and organizational environments. It covers key aspects such as cyber security, various cyber threats, and introduces the ISO 27005 framework for information security risk management. The chapter also delves into the concept of cyber insurance, its coverage, policies, and different insurance programs. Categories of cyber risks are discussed along with case studies illustrating fines and penalties imposed on countries. The chapter concludes by emphasizing the importance of cybersecurity for businesses.

Chapter 3 explores the advantages and limitations of cyber insurance as a risk management tool. It highlights its role in providing financial protection, risk transfer, enhanced incident response, and risk assessment and improvement. The chapter discusses cyber insurance services and coverage, including risk assessment, and provides practical application examples and case studies. It also introduces some well-known cyber insurance companies.

Chapter 4 analyzes the types of information required for risk assessment and insurance coverage. It emphasizes the importance of communication and collaboration between insured parties and insurance companies. The process for applying cyber insurance is detailed, including steps, identification of vulnerabilities, and contract implementation. The chapter also examines the benefits of insurance companies in enhancing cybersecurity for businesses and discusses technological challenges in secure information sharing.

Chapter 5 presents comprehensive guidelines for information technology professionals on selecting, evaluating, and accepting cyber insurance. It underscores the importance of education and awareness among IT professionals.

Chapter 6 outlines an incident response management framework and highlights the collaboration between public and private organizations in addressing cybersecurity incidents. It discusses strategies for effective collaboration and information sharing between these entities

and provides real-life case studies illustrating collaboration concerning cyber insurance and cybersecurity.

Table of Context

Chapter 1 - Introduction

In today's linked and digitally enabled world, businesses and organizations face a widespread and evolving hazard landscape in the form of cyber threats and dangers. Due to the speedy digitization of processes, the increasing reliance on networked systems, and the widespread use of advanced hacking techniques, cybersecurity is quickly becoming one of the most important organizational challenges. It is critical to manage cyber threats and hazards since a successful cyberattack can have a detrimental impact on an organization's operations, reputation, and financial stability (Anderson, J., & Jain, A., 2018).

Due to the extent and frequency of cyber-attacks, a proactive cybersecurity plan is first and foremost necessary. Cybercriminals frequently exploit holes in networks, software, and user behavior to enter a system without authorization.

Every day, cybercriminals — from lone hackers to organized crime groups — exploit weaknesses in networks, apps, and user behavior to access confidential information, stop business operations, or steal money (Everett, 2011). Cyber events can result in significant expenses with long-lasting effects, such as monetary losses, legal responsibilities, and reputational harm.

Additionally, the interconnectedness of the current business environment on a worldwide scale enhances the potential impact of cyber threats. Supply chains, networks for information sharing, and collaboration platforms are becoming crucial elements of contemporary company operations. Any breach within these interconnected ecosystems has the potential to affect numerous enterprises, causing extensive disruption and loss. As a result, dealing with cyber threats has become a shared duty between enterprises, organizations, and their stakeholders, necessitating cooperative efforts to reduce risks and maintain resilience (Farley et al., 2021).

Furthermore, organizations and corporations now must comply with legal obligations as well as industry norms. Globally, governments and regulatory organizations have acknowledged the seriousness of cyberthreats and have enacted strict regulations to preserve private data, safeguard vital infrastructure, and protect privacy. Violations of these rules may incur harsh fines, legal repercussions, and reputational harm to a business. To achieve compliance and uphold stakeholder trust, firms must proactively handle cyber threats (D'Arcy, 2009).

Following the requirements provided in ISO 27005, this Master's Thesis goes deeply into an extensive analysis of the difficulties and factors to be taken into account when using cyber insurance as a supplemental technique for controlling risks in modern corporate and organizational contexts. Given our growing reliance on technology and the evolving threat

landscape of cyber risks, organizations face a pressing need to safeguard their sensitive information and critical assets. In response to these evolving threats, cyber insurance has emerged as a potential solution to mitigate financial losses and provide a layer of protection against cyber incidents.

The objective of this study is to analyze and address the various complexities and implications surrounding the integration of cyber insurance into existing risk management frameworks. By aligning with the principles and practices outlined in ISO 27005, a widely recognized international standard for information security risk management, this research aims to shed light on the potential benefits and challenges of incorporating cyber insurance as part of a holistic risk treatment strategy (Whitman, 2019).

Throughout this thesis, we will explore the multifaceted aspects of cyber insurance, considering its applicability, effectiveness, and limitations in contemporary business and organizational environments. This includes examining key factors such as policy coverage, underwriting considerations, claims management, and the role of insurance providers in promoting cybersecurity awareness and best practices. Additionally, we will evaluate the impact of cyber insurance on risk culture, risk transfer mechanisms, and the overall resilience of organizations in the face of cyber threats.

By digging into these critical aspects, this research endeavors to provide valuable insights and recommendations for organizations seeking to enhance their risk management strategies through the integration of cyber insurance. By combining the expertise and guidance provided by ISO 27005 and the evolving landscape of cyber insurance, organizations can make informed decisions to effectively manage cyber risks while safeguarding their operations, reputation, and financial well-being (Coalition., 2021).

In summary, this Master's Thesis aims to contribute to the understanding and advancement of cyber insurance as a complementary risk treatment option in line with ISO 27005 standards. By exploring the intricacies of cyber insurance and its role in modern business and organizational environments, this research aims to provide practical recommendations and insights to support informed decision-making and foster resilience against cyber threats.

1.1. Introduction to cyber insurance

In today's digital age, businesses and organizations face an ever-increasing array of risks and threats to their information systems and data. The rapid advancement of technology has brought numerous benefits, but it has also exposed vulnerabilities that can be exploited by malicious actors. As a result, organizations are constantly seeking effective strategies to mitigate these risks and protect their valuable assets (Farley et al., 2021).

One approach that has gained significant attention in recent years is cyber insurance. Cyber insurance is a specialized form of insurance designed to help organizations manage the financial consequences of cyber incidents and data breaches. It offers coverage for various aspects, including legal costs, data recovery, public relations, and compensation for third-party losses. By transferring some of the financial risks associated with cyber incidents to insurance providers, organizations can potentially reduce the impact of these incidents on their operations and finances (Farley et al., 2021).

The adoption and application of cyber insurance as a risk management strategy, however, is not without difficulties. This Master's Thesis examines a number of crucial challenges that come up in contemporary corporate and organizational situations when employing cyber insurance as a supplemental risk management alternative, particularly when aligned with the ISO 27005 standard.

Information security risk management is outlined in the widely accepted international standard ISO 27005. It provides a methodical and organized strategy to detecting, evaluating, and managing information security risks. Organizations can benefit from a defined process to evaluate their cyber risks and choose the best risk management strategies, including cyber insurance, by integrating cyber insurance inside the framework of ISO 27005.

Throughout this thesis, we will delve into several key aspects of using cyber insurance in conjunction with ISO 27005. These include the evaluation of cyber risks, the selection of appropriate coverage, the determination of policy limits and exclusions, and the overall effectiveness of cyber insurance as a risk treatment option. By thoroughly examining these issues, we aim to provide valuable insights and recommendations that can guide organizations in their decision-making process regarding cyber insurance adoption and implementation (Isaac., 2023).

1.2 Importance and need for addressing cyber threats and risks in businesses and organizations

Cyber hazards and dangers must be handled due to the potentially disastrous effects they could have on enterprises and organizations. A successful cyberattack may result in significant financial losses, damage to one's reputation, noncompliance with rules, or even the closure of an entire business. Furthermore, because supply networks and commercial alliances are interconnected, a cyber-attack that affects one organization may also damage others.

Additionally, organizations and enterprises are trusted with sensitive data from their partners and clients. This includes financial records, commercial secrets, and personal information. Inadequate security measures might result in privacy violations, a decline in trust,

and legal repercussions. As a result, managing cyber hazards and risks is essential for preserving ethical standards and fulfilling legal obligations in addition to ensuring company continuity (Coalition, 2021).

The changing threat landscape is a significant element in the need to combat cyber risks. Cybercriminals are getting more and more skilled, using cutting-edge methods and equipment to get past security measures. They continually modify their techniques to take advantage of flaws in systems and to use social engineering to prey on human weaknesses. This flexible quality of cyber threats necessitates a proactive and comprehensive approach to risk management, including the adoption of appropriate measures and strategies to mitigate and transfer risks.

Additionally, because modern business ecosystems are interconnected, organizations are also responsible for safeguarding both their own internal systems and the larger network to which they belong. A single network weak spot could jeopardize the ecosystem's security as a whole. In order to effectively manage cyber risks and threats, businesses, industrial sectors, and even governmental entities must coordinate and work together. It is a collective responsibility.

Not to mention, businesses and organizations must demonstrate to their stakeholders their commitment to cybersecurity as the digital landscape changes. Customers and investors are paying more and more attention to cybersecurity for the reasons that were presented earlier in this work.

By effectively addressing cyber threats and risks, organizations can enhance their reputation, attract new business opportunities, and create a competitive advantage in the market (Isaac., 2023).

1.3. Overview of the objectives and structure of the paper

The digital revolution is here to stay, and we shouldn't try to stop it. The key drivers of future growth will be technical advancements, which will provide businesses and organizations with prospects of generating value and a competitive edge. But in order for businesses to prosper in the digital age, they need a solid cyber security plan that will push them to increase their level of security, preparedness, and resilience to cyberattacks. As new technologies contribute to the phenomena known as "digital disruption," they bring new kinds of cyber risks and strengthen those that already exist, necessitating the development of advanced next-generation capabilities right once.

To balance the need to defend themselves from current threats with the need to adopt new business models and new strategies that leverage digital technology and lay the groundwork for growth, organizations must be able to constantly understand the opportunities

and risks associated with digital innovation. To protect themselves from the risks of cyberspace, companies should, in this situation, thoroughly understand their risk profile, evaluate the effectiveness of their current security measures, and set up an all-encompassing Cyber Security program. Cyber risk management is a dynamic process that is always changing and evolving in response to the threat landscape. The portrayal of the development of the cybersecurity environment over the previous years makes it abundantly evident, that a comprehensive strategy that prioritizes prevention, empowers organizations.

Taking into consideration all the above, the research questions that this thesis aims to answer are the following:

- What are the vulnerabilities that today businesses face in their network infrastructure?
- What is the purpose of cyber insurance and what does it cover?
- What are the strategies that private and public sector should follow in order to effectively deal with cyber-attacks?

Chapter 2 - Theoretical background

In the mid-2000s, cyber insurance companies introduced a new type of coverage called first-party expense cyber insurance. This expansion of insurance offerings meant that any company utilizing technology could now be covered. First-party expense cyber insurance aims to reimburse companies for the costs incurred directly from a cyberattack impacting their business. These policies can be tailored to suit the specific needs of each company, covering expenses such as credit monitoring, data breach response, crisis management consultancy, negotiators for ransom payments, and data recovery (Tondel et al., 2019).

Silent cyber risk represents another form of cyber insurance coverage, but it is not a standalone cyber insurance policy. Instead, it refers to potential cyber-related losses arising from traditional property and casualty (P&C) policies that were not explicitly designed to cover cyber risks. An example scenario could be a hotel's computer system getting infected with malware, leading to the activation of the sprinkler system, causing interior damage and maybe an injury due to slipping and falling. If cyber risks are not specifically excluded in the traditional property insurance coverage, it may be expected damages and medical bills derived from such incidents to be covered. However, the concept of silent cyber is gradually diminishing as insurers shift to P&C policies that either include or explicitly exclude losses from cyberattacks. Leading insurers, such as AIG, have taken steps to transition to affirmative cyber coverage, eliminating most silent cyber risks in their business (Granato et al., 2019).

While the cyber insurance market is rapidly growing, it still remains a relatively small segment within the overall U.S. P&C insurance market. Businesses in the U.S. can obtain cyber insurance either as a standalone policy or as part of a bundled package with their general P&C coverage. In 2018, standalone policies accounted for $1.1 billion in premiums, while packaged policies amounted to $922 million. Despite the significant increase in written premiums since 2015, the cyber insurance market's share remains relatively small, comprising less than 0.5% of the total U.S. P&C business OECD (Organization for Economic Cooperation and Development) (2017).

The adoption rates of cyber insurance vary widely across firms and industries. Large businesses show higher adoption rates, with 61% having standalone cyber insurance policies, compared to only 29% of small businesses. Sectors such as education (69%) and healthcare (52%) have the highest adoption rates, while technology and communications firms stand at 51%. On the other hand, industries such as financial institutions (37%), manufacturing (38%), retail (49%), and utilities (31%) exhibit lower adoption rates. These differences in adoption rates suggest that cyber insurance awareness and acceptance vary depending on the size and industry of the businesses involved (Granato et al., 2019).

2.1. Analysis of cyber threats and risks in modern business and organizational environments

2.1.1 Cyber Security

There are several definitions about cyber security. In the insurance industry, certain definitions have been given, some of them will be mentioned below.

Chief Risk Officers of insurance companies (CRO Forum, 2014) define cyberspace as a risk that includes any risks arising from the use and transmission of electronic data, including technological tools such as the internet and telecommunications networks.

The Geneva Association (2016), a major insurance sector body gives a similar definition: cyber risk includes any risk arising from the use of information and communication technology that compromises the confidentiality, availability or integrity of data or of the services offered.

Both of these definitions generally include risks associated with the use of information and communications technologies, which may include risks arising from human error or intentional/malicious attacks, whether from internal or external sources (such as nation states, terrorists, industrial competitors, organized crime, hackers/criminals). The Geneva Association definition is particularly useful as it delineates risk within the internet and incidents that may lead to a data breach (Malyuk, 2016).

Information security professionals face significant challenges due to the dynamic nature of cyber risks and threats in modern corporate and organizational environments. Understanding the nature and scope of these threats is crucial for efficient prevention and management of cyber hazards. The main cyber risks and hazards that businesses and organizations are currently facing will be examined in this analysis (Franke, 2017).

One noteworthy cyber risk is the frequency of data breaches. Attackers target businesses in an effort to gain unauthorized access to personal information, financial records, intellectual property, and other types of confidential data. In addition to causing financial losses, data breaches can have major consequences for the people who are affected, like fraud and identity theft. Analyzing data breaches requires the use of analysis of data breaches which involves examining attack vectors, vulnerabilities in systems, and the effectiveness of security controls (Isaac., 2023).

Ransomware attacks are a serious cyberthreat. Ransomware encrypts data belonging to an organization and then, makes it unavailable unless a ransom is paid. Such attacks have the

potential to stop operations, interfere with services, and cause serious financial and reputational harm. Understanding attack vectors, the development of ransomware variations, and the efficacy of incident response and recovery measures are all important considerations when analyzing ransomware risks (Droppa et al., 2021).

Social engineering and phishing attacks are two more serious cyberthreats. These assaults make use of weaknesses in people and trick them in order to disclose sensitive information or take actions that jeopardize security. Attackers frequently use phishing emails, bogus websites, and false phone calls. Examining attack methods, employee awareness and training programs, and other factors are necessary for analyzing phishing and social engineering threats (Droppa et al., 2021).

Cloud services and the Internet of Things (IoT) are used more often. Therefore, in this case vulnerabilities are presented. Scalability and flexibility are two advantages of cloud computing, but it also poses issues with data protection, security measures, and the potential for illegal access. Similar to how smart home gadgets can be hacked to launch attacks or obtain unauthorized access to networks, IoT devices, which include everything from industrial control systems to smart home devices, increase the attack surface. Threats associated to the cloud and IoT can be analyzed by evaluating security measures, encryption procedures, and vulnerability management (Woldemichael, 2020). Additionally, corporations face a serious danger from insider attacks. Insiders, such as staff members, independent contractors, or business partners, may inadvertently or purposefully jeopardize security by performing operations like unauthorized data access, data theft, or sabotage.

The regulatory environment also adds another level of complexity to cyber risks and attacks. Organizations have to manage a bunch of compliance regulations, such as California Consumer Privacy Act (CCPA) or the General Data Protection Regulation (GDPR). These restrictions carry substantial penalties and reputational risks for noncompliance. Assessing the organization's compliance with pertinent legislation, data governance procedures, and the efficacy of compliance monitoring and reporting mechanisms are all part of the regulatory risk analysis process (Mulugeta, 2023).

Analyzing cyber risks and hazards in current corporate and organizational environments is crucial for the creation of effective cybersecurity policies. By comprehending the nature and scope of these threats, organizations may implement the proper security measures, develop incident response strategies, and allocate resources effectively to reduce cyber dangers. To keep ahead of new threats and guarantee that businesses and organizations are resilient in the face of developing cyber hazards, constant monitoring and analysis of the threat landscape are crucial.

2.1.2 Most known cyber threats

Information security faces several, well-known cyber hazards and threats in contemporary corporate and organizational environments. The following are a few of the more frequent and well-known threats:

Ransomware and malware

Network system and computers can be infected by malicious software (malware) and ransomware, which encrypts data and demands a fee in exchange for release. In that case, critical operations may be stopped and most importantly there may be data loss or theft. Moreover, there may be monetary damages. Cyber dangers like malware and ransomware, which are quite common and dangerous, can have serious repercussions for enterprises and organizations (Junior, 2023).

Malicious software that is intended to infiltrate and compromise computer systems is referred to as malware. It can spread through hacked software downloads, fraudulent websites, or email attachments. Once installed, malware can perform a range of malicious activities, such as stealing sensitive data, damaging or deleting files, and gaining unauthorized access to systems. Malware attacks can lead to significant disruption of operations, loss of productivity, financial losses due to remediation efforts, and compromised data security.

Because enterprises might not be able to access crucial information and systems until the ransom is paid or the data is restored in some other way, ransomware attacks can cause significant harm and inconvenience. In addition to the ransom payment itself, ransomware attacks may result in possible revenue losses owing to downtime, reputational harm, legal ramifications, and incident response and recovery costs (Junior, 2023).

Attacks involving malware and ransomware both have the potential to steal or lose data, which has serious repercussions for organizations. Loss of confidential or sensitive information can have negative effects on reputation, legal trouble, financial penalties, and regulatory non-compliance. Further harm to those impacted can result from stolen data being used for identity theft, fraud, or selling on the dark web.

Malware and ransomware attacks can cause significant financial losses. Organizations may have to pay for forensic investigations, data restoration, system cleanup, and legal or regulatory compliance as part of incident response and recovery costs. During the recovery phase, productivity losses and business interruptions can both have a major financial impact. In order to stop future attacks and fortify their defenses against malware and ransomware threats, enterprises may also need to invest in improved security measures and cybersecurity solutions (Mulugeta, 2023).

Organizations should use a multi-layered strategy to cybersecurity to reduce the dangers brought on by malware and ransomware. This entails putting in place reliable antivirus and anti-malware software, upgrading programs and systems often to fix bugs, training staff members to spot and avoid hazardous information, and creating safe data backups. Therefore, organizations should develop incident response plans to effectively manage and recover from malware and ransomware attacks, including communication protocols, backup restoration processes, and engagement with law enforcement, if necessary.

Phishing and Social Engineering

Phishing attacks involve deceptive tactics, such as fraudulent emails or websites, to trick individuals into revealing sensitive information or performing actions that compromise security. Social engineering techniques exploit human vulnerabilities to manipulate individuals into divulging confidential information or granting unauthorized access (Dogan et al, 2022).

Vulnerabilities of Internet of Things (IoT)

Smart devices, such as smart home devices, industrial control systems lack robust security controls, making them susceptible to exploitation. Compromised IoT devices can be used to launch attacks or gain unauthorized access to networks.

Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service (DDoS) attacks are a malicious technique used to overwhelm and disrupt the functioning of online services, websites, or networks. In a DDoS attack, a vast network of compromised computers, often referred to as a botnet, is coordinated by cybercriminals to flood a target system with an enormous volume of traffic or requests. The objective is to saturate the target's resources, such as bandwidth, processing power, or memory, rendering it incapable of serving legitimate users' requests. These attacks can vary in scale and sophistication, and they pose significant threats to organizations of all sizes, from small businesses to large enterprises.

DDoS attacks can have severe consequences, including financial losses, reputational damage, and potential data breaches. They can disrupt online services, making them inaccessible to customers, which can result in revenue loss and customer dissatisfaction. Furthermore, DDoS attacks can serve as a smokescreen for more targeted cyberattacks, diverting the attention of security teams while attackers exploit vulnerabilities elsewhere in the system.

Insider Threats

Insiders, including employees, contractors, or business partners, pose a risk to organizations by intentionally or unintentionally compromising security. This can involve unauthorized data access, data theft, or sabotage of systems and networks.

Insider threats represent a significant and complex challenge for organizations, as they involve individuals who have authorized access to systems, data, and sensitive information. Insiders, including employees, contractors, or business partners, can intentionally or unintentionally compromise security, leading to potential harm to the organization.

Intentional insider threats occur when individuals abuse their access privileges to engage in malicious activities. This can include unauthorized data access, stealing sensitive information for personal gain, or carrying out acts of sabotage against the organization's systems, networks, or reputation. Motivations for intentional insider threats may vary, such as financial gain, revenge, ideological reasons, or coercion by external entities (Saxena et al., 2020).

On the other hand, unintentional insider risks are caused by mistakes made by individuals, a lack of knowledge, or insufficient training. Employees or others working for the company may unintentionally fall victim to social engineering tricks like phishing emails or fake websites, leading to accidental data breaches or illegal access to systems. Unintentional insider risks can also result from careless actions, such as handling confidential information carelessly, using weak passwords, or disobeying set security standards.

Organizations may suffer serious repercussions as a result of insider threats. They may result in unlawful disclosure of private data, intellectual property theft, compromise of vital systems, interruption of business operations, monetary losses, failure to comply with legal and regulatory requirements, harm to reputation, and loss of consumer trust. Insider risks can also be difficult to identify because they frequently have legitimate access to systems and may intentionally try to evade detection (Saxena et al., 2020).

To mitigate insider threats, organizations should implement a comprehensive approach to insider risk management. This involves several key elements:

1. Access Control and Least Privilege: Implementing strong access controls and ensuring that individuals only have access to the systems and data necessary for their roles can help minimize the potential for unauthorized activities.

2. Employee Training and Awareness: Regular training programs on cybersecurity best practices and awareness campaigns can educate employees about the risks associated with insider threats, the importance of data protection, and the consequences of negligent or malicious actions.

3. Monitoring and Behavioral Analytics: Implementing monitoring systems and utilizing behavioral analytics can help identify suspicious activities, such as unusual data access patterns, unauthorized data transfers, or abnormal user behavior that may indicate insider threats.

4. Incident Response and Reporting: Establishing clear incident response procedures and mechanisms for employees to report potential insider threats anonymously or confidentially encourages a culture of accountability and helps detect and respond to threats in a timely manner.

5. Insider Risk Assessment and Continuous Monitoring: Conducting periodic risk assessments to identify vulnerabilities, implementing regular audits, and monitoring insider activities can help proactively detect potential insider threats and take appropriate preventive measures.

6. Trustworthy Workforce Culture: Promoting a culture of trust, transparency, and open communication within the organization can foster an environment where employees feel comfortable reporting suspicious activities and addressing potential concerns related to insider threats.

By adopting a comprehensive insider risk management strategy, organizations can better protect their systems, data, and assets from the detrimental impacts of both intentional and unintentional insider threats.

APTs, or advanced persistent threats

APTs are highly advanced, specifically targeted cyberattacks that are conducted over time by knowledgeable adversaries. They want to exfiltrate private information, interfere with operations, or obtain illegal access to networks. APTs frequently use a mix of malware, social engineering, and other techniques to avoid detection. APTs are among the most intricate and sophisticated cyberattacks that organizations today are subjected to. APTs are frequently conducted by well-resourced and highly competent adversaries, such as nation-states or organized cybercrime gangs, with clear objectives and lengthy operational schedules (Hejase, 2020).

APTs take a more deliberate and strategic approach than regular cyberattacks. APTs strive to sustain long-term access to targeted networks, exfiltrate important information, or disrupt crucial operations rather than making fast compromises. These attacks have a number of important traits.

1. Advanced Methods: APTs use cutting-edge methods to avoid detection and get beyond conventional security measures. In order to take advantage of weaknesses

and utilize fresh attack vectors, they constantly modify their tactics, methods, and procedures (TTPs). To acquire initial access to networks, APTs may use bespoke malware, zero-day exploits, or cutting-edge social engineering techniques (Hejase 2020).

2. Consistency and endurance: APTs are persistent in their operations and may go unnoticed for long stretches of time, sometimes lasting months or even years. Adversaries methodically plan and carry out their attacks, lateralizing via the network, upgrading privileges, and keeping a foothold to accomplish their goals covertly (Cinar, 2018).

3. Targeted Strategy: APTs deliberately target businesses, sectors, or even individuals who have access to sensitive and valuable data. Adversaries carry out extensive reconnaissance to obtain information about the target's resources, personnel, and security measures. They can thus customize their attacks to take advantage of particular flaws and increase their chances of success.

4. Coordinated Campaigns: APTs often involve multiple stages and coordinated actions to achieve their goals. Initial compromise may occur through tactics like spear-phishing emails, watering hole attacks, or supply chain compromises. Once inside the network, adversaries establish persistence, conduct reconnaissance, and exploit vulnerabilities to move laterally, escalate privileges, and exfiltrate valuable data.

5. Stealthy Exfiltration: APTs prioritize stealth when exfiltrating sensitive data. They employ encryption, steganography, or covert communication channels to evade detection and minimize the chances of being detected by security monitoring systems. This allows them to maintain a persistent presence while quietly exfiltrating valuable information over time.

Defending against APTs requires a multi-layered and proactive security approach. Organizations can employ the following measures:

1. Security Intelligence: Keep up with new APT campaigns, TTPs, and indicators of compromise (IOCs) by routinely monitoring and analyzing threat intelligence sources. This aids in the quick detection and reaction to any APT activity.

2. Endpoint Security: Deploy modern endpoint security tools that take advantage of threat intelligence, machine learning, and behavioral analysis to spot and stop APT-related activity on specific devices.

3. Network segmentation: Utilize network segmentation to separate vital systems and prevent lateral network migration. This limits the potential impact of APTs and aids in keeping the attack from spreading further.

4. IDS/IPS: Utilize reliable intrusion detection and prevention systems (IDS/IPS) that track network traffic and look for unusual activity that could be an APT. Real-time detection and blocking of questionable activity is possible with these technologies.

5. Employee Education and Awareness: Inform staff members on APTs, social engineering strategies, and the value of adhering to security best practices. Employees who receive regular training can identify and report odd behaviors that could be signs of APT activity.

6. Incident Response and Recovery: Create a thorough incident response plan that details how to identify, stop, and recover from APT occurrences. These cover containment techniques, system restoration techniques, and forensic analysis techniques (Saxena et al., 2020).

Organizations can increase their resistance to APTs and lessen the potential harm posed by these sophisticated and focused cyber-attacks by putting these preventative security measures into place and preserving a solid security posture. Organizations may keep ahead of developing APT operations and safeguard their crucial assets by conducting regular security assessments, penetration testing, and working closely with cybersecurity professionals.

Data Breaches

Data breaches involve unauthorized access or exposure of sensitive or confidential information, including personal data, financial records, or intellectual property. Data breaches can lead to severe financial losses, reputational damage, and regulatory non-compliance.

Data breaches are more frequent in contemporary commercial and organizational settings, posing serious hazards to the privacy, accuracy, and accessibility of sensitive data. A data breach happens when unauthorized people or organizations access secured data, potentially harming both people and organizations (Singh, 2022).

Data breaches can have serious repercussions on an organization's financial and non-financial aspects:

1. Financial Losses: Organizations may suffer significant financial losses as a result of data breaches. These losses may result from a number of things, such as incident response expenses, legal expenditures, regulatory fines, prospective legal action,

and paying harmed parties for losses. Along with brand harm, client attrition, and lost commercial possibilities, firms may also see a drop in revenue.

2. Reputational Damage: Data breaches can seriously damage a company's reputation and destroy stakeholders' and consumers' trust. Inadequate handling of sensitive information and security flaws can result in unwanted media attention, public scrutiny, and a decline in trust. in the organization's ability to protect data. Rebuilding a damaged reputation can be a long and challenging process.

3. Compliance violation: General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are some examples of laws that have been passed in various countries to regulate data protection and privacy. Regulation violations can cost an organization more money and further harm its brand (Naseer, 2016).

4. Operational and Legal Consequences: Among other legal ramifications, data breaches may give rise to class action lawsuits, individual damage claims, and contractual disputes. Organizations may also incur operational disruptions as a result of a breach, such as system failures, lost productivity, or delayed business processes.

5. Identity Theft and Fraud: In the aftermath of a data breach, stolen personal information can be exploited for identity theft, financial fraud, or other malicious activities. This can harm individuals whose data was compromised and lead to financial losses, emotional distress, and damage to credit histories.

To mitigate the risks associated with data breaches, organizations should implement a comprehensive approach to data protection and security. Organizations should adopt a thorough strategy for data protection and security in order to reduce the risks related to data breaches (Singh, 2022):

a. Strong Security Controls: Data can be protected from unwanted access by combining technological and organizational security methods such access controls, encryption, firewalls, intrusion detection systems, and safe coding techniques.

b. Compliance with data governance and privacy laws: Organizations can build effective data protection procedures by putting data governance frameworks into place and following pertinent privacy rules. This entails doing data inventories, establishing data classification, and making sure that data handling procedures adhere to statutory and industry standards.

c. Employee Education and Awareness: Employees should be made aware of the value of data protection, the need to handle sensitive data securely, and the need to identify and report any security incidents. Training programs can help foster a security-conscious culture and reduce the likelihood of human error leading to data breaches.

d. Incident Response Planning: It's essential to create a strong incident response plan that details what to do in the case of a data breach. This covers procedures for spotting and containing security breaches, getting in touch with those affected, working with law enforcement, and starting recovery and remedy actions.

e. Risk Management of third-party companies: In most cases, third-party vendors and partners frequently have access to sensitive data, it is crucial to evaluate their security procedures. To safeguard shared data and reduce the risk of breaches coming from third parties, organizations should make sure that the right security measures and contractual agreements are in place.

By adopting these proactive measures and continually assessing and improving their security posture, organizations can enhance their ability to prevent, detect, and respond to data breaches effectively. Protecting the privacy and security of sensitive information must be an ongoing priority to mitigate the potentially devastating consequences of data breaches.

Supply Chain Attacks

Supply chain attacks target vulnerabilities in third-party vendors or suppliers to gain unauthorized access to the target organization's systems. Attackers exploit trusted relationships to inject malware, compromise software updates, or tamper with hardware. Supply chain attacks have emerged as a significant and growing threat to organizations, highlighting the interconnected nature of modern business ecosystems. These attacks exploit vulnerabilities in third-party vendors or suppliers to gain unauthorized access to the systems and data of target organizations. Attackers leverage trusted relationships, compromising the supply chain to infiltrate and compromise the target's security defenses (Naseer, 2016).

Supply chain attacks can take various forms and involve different attack vectors:

1. Malware Injection: Attackers may inject malicious code or malware into the software or firmware supplied by a vendor. This can occur during the development process or through compromised software updates. When organizations unknowingly install or integrate the compromised software or updates, the malware gains a foothold in their systems, allowing attackers to execute their malicious activities.

2. Software Supply Chain Compromise: Attackers may compromise the development or distribution process of a software vendor, introducing unauthorized modifications or backdoors into the software. Organizations unwittingly install and use the compromised software, which provides an entry point for attackers to exploit.

3. Hardware Tampering: Supply chain attacks can also involve tampering with hardware components during the manufacturing or distribution process. Attackers may implant malicious components or modify legitimate hardware to enable unauthorized access or surveillance. Compromised hardware may be integrated into an organization's infrastructure, leading to vulnerabilities that can be exploited by attackers.

4. Vendor Account Compromise: Attackers may target vendor accounts to gain unauthorized access to the vendor's systems or sensitive data. Once inside, they can manipulate the vendor's software or systems, introduce malicious code, or gather intelligence that facilitates further attacks on the target organization.

Supply chain attacks can have significant consequences for organizations. One of the most severe consequences is the unauthorized Access. In this case, attackers gain access to the target organization's systems, networks, and sensitive data, which can lead to data theft, intellectual property theft, or unauthorized activities within the compromised environment. Another important consequence is data Compromise. On this case, a compromised supply chain component can expose sensitive information, such as sensitive customer data, financial reports, or other sensitive data. This can result in financial losses, regulatory non-compliance, reputational damage, and legal repercussions.

Moreover, there is a like hood of disruption of Operations. Malicious users, may disrupt business operations, causing system downtime, loss of productivity, and service disruptions. This can lead to financial losses, customer dissatisfaction, and may harm business relations with its customers.

Last but not least, an organization may be harmed in means of reputation. Public exposure of a supply chain attack can tarnish an organization's reputation and impact its competitiveness in the marketplace.

To mitigate the risks associated with supply chain attacks, organizations should consider the following measures:

1. Vendor Risk Management: Implement robust vendor risk management programs to assess and monitor the security practices of third-party vendors and suppliers. This includes conducting due diligence, evaluating their security controls, and

establishing contractual obligations regarding cybersecurity standards and incident response protocols.

2. Secure Development Lifecycle: Encourage vendors to follow secure development practices, such as conducting code reviews, implementing secure coding standards, and performing thorough testing to detect and prevent vulnerabilities in their software or firmware.

3. Multi-Factor Authentication (MFA): Enforce the use of MFA for vendor accounts and privileged access to critical systems, reducing the risk of unauthorized access in the event of a compromised account.

4. Supply Chain Audits: Regularly audit and review the security controls and processes of vendors and suppliers to ensure compliance with established standards and best practices.

5. Incident Response Preparedness: Develop an incident response plan that specifically addresses supply chain attacks. This plan should include procedures for detecting and responding to such attacks, communicating with affected parties, and implementing recovery measures.

6. Continuous Monitoring and Threat Intelligence: Implement robust monitoring systems and leverage threat intelligence sources to detect and respond to emerging supply chain attack techniques, indicators of compromise, or vulnerabilities in vendor software or hardware.

By implementing these proactive measures, organizations can strengthen their supply chain resilience, reduce the likelihood of supply chain attacks, and effectively mitigate the potential impact of such attacks. Collaborating closely with vendors, maintaining clear lines of communication, and fostering a security-focused culture throughout the supply chain can also contribute to a more secure and resilient business ecosystem.

Zero-Day (0-Day) attack

Zero-day exploits are flaws in software or systems that the vendor is unaware of and has not patched. Before they are found and fixed, cybercriminals take advantage of these vulnerabilities to launch specialized attacks. Today, zero-day exploits are one of the most harmful attacks for organizations and refer to software or system flaws that the vendor is unaware of and for which there is no patch or security update. Due to this information gap, cybercriminals have a distinct advantage since they can use these hidden vulnerabilities to

launch sophisticated, targeted assaults before the manufacturer is made aware of the problem and issues a fix (Franklin et al., 2022).

Zero-day vulnerabilities can be found using a variety of techniques, such as independent study, clandestine forums, or specialist hacker teams. Cybercriminals spend time and resources creating exploit code to take advantage of a vulnerability once it has been found in the program or system. With the aid of this exploit code, they are able to circumvent security barriers and get access to certain systems without authorization (Franklin et al., 2022).

The limited ability to be detected by zero-day exploits is one of their worrying characteristics. In order to recognize and stop attacks, traditional security measures like antivirus software or intrusion detection systems sometimes rely on recognized signatures or patterns of harmful activity. Zero-day exploits are difficult to detect until after they have been used because they elude these traditional detection measures since they take advantage of previously undiscovered vulnerabilities.

The consequences of zero-day exploits can be severe for organizations. Cybercriminals exploit these vulnerabilities to carry out targeted attacks against specific organizations or individuals. By using an undisclosed vulnerability, attackers can bypass existing security measures and gain unauthorized access to sensitive information, systems, or networks. This unauthorized access can lead to data theft, financial losses, reputational damage, and legal consequences (Von., 2013).

2.2. Description of the ISO 27005 framework for information security risk management

Information security risk management is governed by the international standard ISO 27005. The ISO 27005 standard, which was created by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), provides a methodical and structured approach to detecting, evaluating, and managing risks associated with information security (Ghazouani, 2023). Helping enterprises create a strong risk management framework for information security is the main goal of ISO 27005. Organizations can efficiently detect and manage potential risks, lessen vulnerabilities, and shield their priceless assets from attacks by putting the principles and procedures specified in the standard into practice (Abdelwahab et al., 2022).

The risk management approach used by ISO 27005 has several important steps. These phases consist of:

1. Risk Assessment Context Establishment: This stage involves defining the scope and context of the risk assessment, including identifying the assets to be protected, the business processes involved, and the applicable legal, regulatory, and contractual requirements.

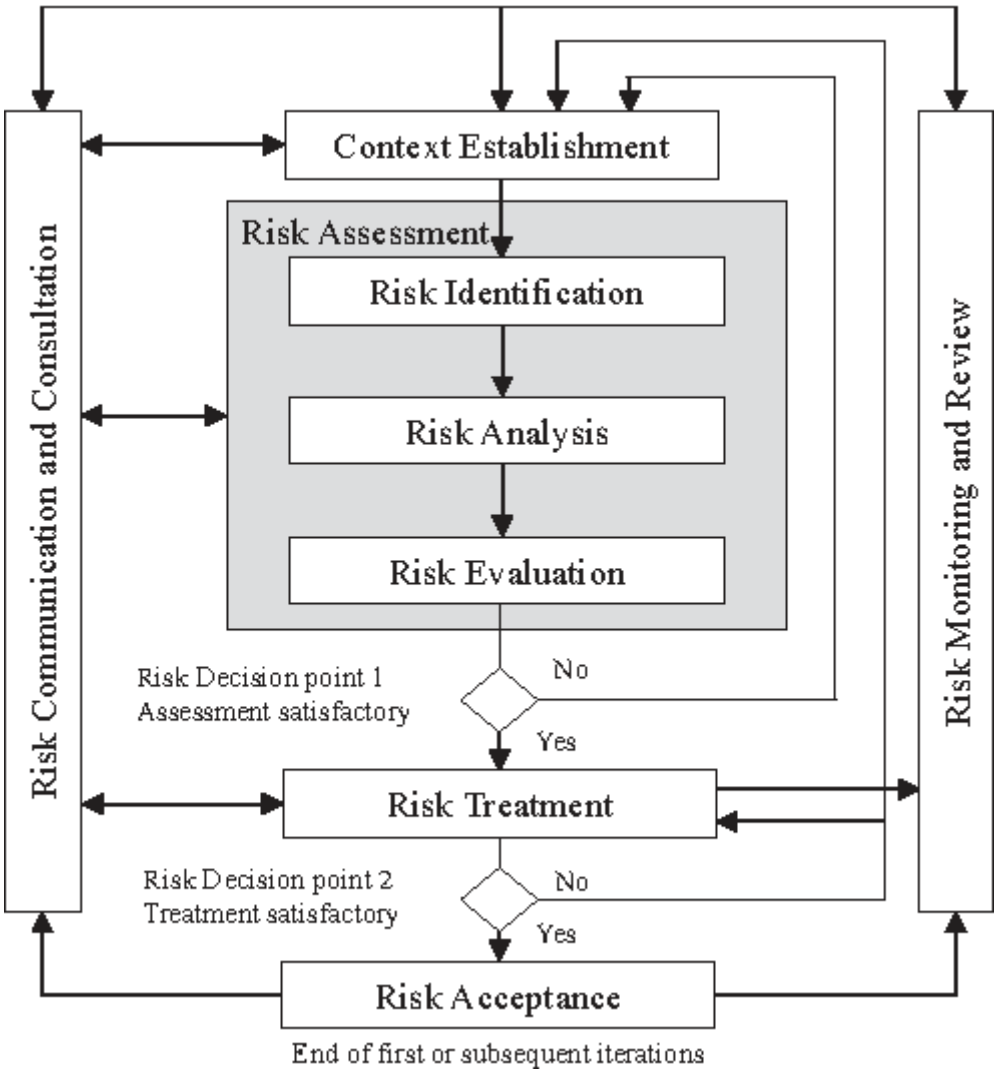
2. Risk Assessment (Identification & Analysis): In this stage, organizations systematically identify and analyze potential risks to their information assets. It involves assessing the likelihood of threats exploiting vulnerabilities and the potential impact of those risks on the organization's objectives.

3. Risk Evaluation: Once risks are assessed, they need to be evaluated to determine their significance and priority. This stage involves considering factors such as the business impact, legal and regulatory requirements, and the organization's risk appetite to make informed decisions about risk treatment.

4. Risk Treatment: Risk treatment is choosing and putting into action appropriate steps to reduce, transfer, avoid, or accept the risks that have been identified. Based on the organization's risk management strategy and goals, this step tries to lower overall risk to an acceptable level.

5. Risk Acceptance: Depending on the organization's risk appetite and the cost-benefit analysis of applying particular measures, some risks may be judged acceptable. Accepting hazards entails consciously deciding to put up with them without additional treatment.

6. Risk Communication and Consultation: The risk management process depends heavily on effective communication and consultation. At this step, risk-related information is shared, stakeholders are consulted, and it is made sure that everyone concerned is informed of the risks, their potential effects, and the selected course of action.



The ISO 27005 standard places a strong emphasis on the value of incorporating risk management into the entire governance structure and decision-making procedures of the business. By encouraging a culture of risk awareness, continuous improvement, and responsibility throughout the business, it encourages a proactive approach to information security.

Organizations may improve their capacity to safeguard sensitive data, abide by legal obligations, and lessen the effects of possible security events by complying to ISO 27005. The standard offers a thorough framework that enables businesses to methodically evaluate and manage information security threats, thereby enhancing the organization's overall security and resilience (Abdelwahab et al., 2022).

2.2.1 Cyber risks - Categories

There are various suggestions as to how the various cyber threats and risks can be categorized. A proposed categorization is this of CRO Forum (2016). According to this categorization main threats and risks are categorized into the following categories:

- Breach of data confidentiality
- System malfunction/problem
- Data Integrity/Availability
- Malicious activity

In this section, the above categories are analyzed and examined, giving specific examples of hacking and online risks (hypothetical/real-world scenarios) will be presented. It is important to note that the CRO Forum (2016) classification is evolving based on incident reporting and attempts to incorporate commonly used security incident and threat reporting metrics such as "VERIS" and "STIX".

Cyber incidents & losses

Cyber incidents have the potential to result in various types of damage, including damage to tangible or even intangible assets. Also, the forms of responsibility to customers, suppliers, employees, shareholders and others, the trust and the relationship of a company with its customers or suppliers are also considered losses. The CRO Forum (2016) has developed a set of “incident type groups” that categorize the losses a company may incur from a cyber-attack.

Below will be mentioned the most important categories of incidents from financial and material losses as well as losses of intangible assets such as reputation and trust, which come from internet attack incidents (Malyuk, 2016):

- Business Process Interruption: Compensation for lost profits resulting from production interruption without material damage
- Contingent Business Interruption (CBI) without physical damage: Compensation for lost profits to the observed company due to production interruption by connected third parties (e.g., suppliers, partners, providers, customers) without physical damage (Avinash et al., 2021).
- Data and Software Loss: Costs associated with recovering, replacing, restoring or replicating lost, damaged, stolen, deleted or encrypted data and software

- Financial Theft and Fraud: Net financial losses resulting from malicious cyber activities, whether internal or external, aimed at committing fraud or stealing financial assets (eg stocks). This coverage includes damages or losses arising from the insured company or caused by third parties to the insured company. Damages or losses should be disclosed (Kshetri, 2018).
- Ransom and cyber extortion: Cost for an expert to handle ransom and extortion incidents, along with payment of ransom (eg, data access held hostage until ransom is paid)
- Infringement or theft of intellectual property: This category includes incidents related to the unauthorized use of intellectual property that lead to financial losses for a company.
- Incident Response Cost: Refers to the financial compensation to handle various incidents. The cost of responding to attack incidents is intended to cover third party companies or external partners, but excludes the cost of covering regulatory and legal defense costs. This coverage includes (Avinash et al., 2021):
    i. IT investigation and forensic analysis (excluding those directly related to regulatory and legal defense costs),
    ii. Public Relations and Communications Expenses,
    iii. Costs of remediation (e.g., costs of removing harmful content posted to insureds).
- Reimbursement for the Negative Impact on Business Operations Arising from Eroded Trust: This entails compensating for the decline in business profits stemming from reduced business activity or customer loss caused by a decrease in confidence in the observed company (Kshetri, 2018).
- Coverage for Expenses Incurred in Regulatory Defense: This pertains to the reimbursement of expenses borne by the observed company or related parties when confronted with investigations by regulatory or governmental bodies related to cyber-attacks. This coverage encompasses legal, technical, or forensic IT services directly associated with regulatory inquiries but excludes any fines or penalties.
- Financial Support for Legal Defense Costs: This involves covering the legal expenses incurred by the observed company or related parties when involved in legal proceedings in court due to cyber-attacks.

- Reimbursement for Monetary Penalties: These addresses compensating the observed company for fines and penalties imposed on it. Reimbursement for these costs is provided only in jurisdictions where it is legally allowed, in accordance with the insights (Kshetri, 2018).
- Compensation for Expenses Related to Communication and Media Liability: This encompasses covering the costs incurred due to the misuse of communication media that results in defamation, slander, or harm to third parties. This includes instances of online defamation, as well as infringements on patents, copyrights, and misappropriation of trade secrets (Blanke, 2019).
- Legal Safeguard - Attorney Fees: Expenses associated with legal proceedings involving the insured party, encompassing attorney fees and court costs in case of litigation. This includes scenarios like identity theft and the legal fees required to establish the misuse of the victim's identity.
- Supportive Assistance - Psychological Aid: Assistance and emotional support for individuals affected by a cyber incident that involves the unauthorized dissemination of damaging information.
- Product-Related Costs (Liability): Reimbursement for costs incurred if products or services provided by the observed company prove to be faulty or cause harm as a result of a cyber incident. This excludes technical products and services (Technological Errors and Omissions) as well as errors and omissions in Professional Services.
- Directors and Officers (D&O) Protection (Liability): Coverage for indemnification expenses in cases where third parties file claims against the company's directors and officers, alleging breach of trust or duty stemming from a cyber-attack.
- Technological Errors and Omissions (E&O) (Liability): Compensation for costs associated with the inability to deliver adequate technical services or technical products due to a cyber incident.
- Professional Services Errors and Omissions (E&O)/Professional Indemnity (Liability): Coverage for indemnity expenses arising from the inability to provide adequate professional services or products due to a cyber incident, excluding technical services and products (Technological Errors and Omissions), as detailed in Blanke's 2019 insights.
- Environmental Harm: Reimbursement for expenses incurred as a result of the release of toxic or polluting substances due to a cyber incident.

- Destruction of Tangible Assets: Losses connected to the physical property of the company that are incurred due to a cyber incident, including disruptions to business operations and potential business interruptions.
- Personal Injury and Loss of Life: Compensation costs for bodily injury or loss of life resulting from wrongful acts or negligence on the part of the observed company or related third parties, such as the disclosure of sensitive data leading to suicide.

2.2.2 Case studies - Fine and Penalties to countries

Data confidentiality breaches, which encompass unauthorized access to personally identifiable information, may trigger notification and/or disclosure requirements in numerous countries. Several noteworthy data breach incidents resulting in fines and penalties in various countries have been documented (Aziz et al., 2020):

In the United States, there exist prompt notification mandates at the state level in nearly all states, with the exception of just three. Furthermore, federal privacy regulations necessitate mandatory notification, both to regulatory authorities and affected individuals, in cases involving the theft of healthcare or financial information. Additionally, the SEC (US Securities and Exchange Commission) mandates disclosure by publicly traded companies in the event of cyber incidents that could substantially impact their financial performance.

Within the European Union, notification requirements are presently less prevalent but are anticipated to change with the implementation of the General Data Protection Regulation (GDPR), which became effective in May 2018. The GDPR mandates obligatory notification to the appropriate supervisory authority when there is a risk to individuals' rights and freedoms concerning their personal data. It also imposes administrative fines in cases of violations deemed intentional or negligent (Aziz et al., 2020).

Concerns of considerable significance revolve around potential harm to assets resulting from cyberattacks within the business technology sector. There are ongoing apprehensions about potential losses stemming from cyberattacks that target control systems and critical infrastructure such as electricity, water, and communication networks.

Moreover, the energy sector is frequently linked to numerous cyberattacks. For instance, the United States Cyber Emergency Response Team noted an increase in incidents affecting industrial control systems in 2015 compared to 2012. Notably, there have been instances of attacks causing physical damage, often due to malware infections or remote access:

- In 2008, a pipeline explosion occurred in Turkey due to a cyberattack that elevated crude oil pressure and disrupted communication systems.

- In 2010, malware was discovered in centrifuges in Iran.
- In 2014, a cyberattack on a steel plant in Germany disabled the blast furnace.
- In 2015, an attack in Ukraine resulted in the disconnection of substations and power loss for thousands of residents.

In addition, there are scenarios that predict potential large-scale damage to industrial control systems, which can be caused by cyber-attacks that cause power outages. These scenarios estimate economic impacts ranging from billions of US dollars, with insured losses potentially reaching trillions of US dollars. These losses will affect business sectors such as power generation and property, with consequences for the economy and insurance claims (Aziz et al., 2020).

2.3. The importance of cybersecurity for business

Up to this point, businesses have diligently secured insurance coverage for their tangible assets and personnel, aiming to safeguard their sustainability. However, the contemporary landscape of communication, globalization, and the rapid evolution of the internet, encompassing the internet of things and big data, has introduced a new peril - the vulnerability of electronic data. Hence, the necessity for Cyber Risk Insurance arises (Iguer et al., 2014).

Frequently, we encounter instances where hacker groups develop malicious software or issue threats against companies, typically with the intent to illicitly access their files. Their motives often involve extorting money, tarnishing the company's reputation, disrupting its operations to inflict financial harm, and more.

The recent European regulation GDPR 679/2016, effective since May 25, 2018, pertains to the compliance requirements and protective measures for personal data held by businesses. It stipulates the potential for claims and demands from third parties in cases of personal data breaches on the internet, entailing penalties of up to 4% of a company's annual revenue and/or fines (as elucidated by Carlton in 2017).

2.3.1. Explanation of the concept of cyber insurance and its various aspects

Cyber insurance or data breach insurance, is a specialized form of insurance designed to help organizations manage the financial consequences of cyber incidents and data breaches.

It provides coverage for various aspects related to cybersecurity and data protection, offering financial protection and support in the event of a cyber incident.

Coverage

Cyber insurance policies typically offer coverage for a range of potential losses and expenses incurred due to a cyber incident (ref. §2.2.1). This can include (Mishra et al., 2022):

- First-party coverage: This covers the direct losses and expenses incurred by the insured organization. It may include costs related to data breach response, forensic investigations, data recovery and restoration, business interruption, and public relations and crisis management.
- Third-party coverage: This covers liability and legal costs arising from claims made by third parties affected by a cyber incident. It may include costs related to legal defense, settlements, regulatory fines, and compensation for third-party losses such as customer notification, credit monitoring, and identity theft recovery.
- Multimedia liability coverage: This covers claims related to defamation, copyright infringement, or unauthorized use of intellectual property in electronic media.

Silent coverage insurance

Several consequences of a cyber incident may already fall within the scope of coverage provided by the insured's existing insurance policies. For instance, if a cyber incident leads to a physical event like a fire or explosion, these damages might be addressed by standard property insurance policies rather than specialized cyber insurance. It's essential for the insured to carefully evaluate the extent of cyber risk coverage within their current insurance portfolio. This assessment should include examining any potential gaps or exclusions related to cyber risks in their existing policies. Additionally, the insured should assess whether their liability insurance coverage is adequate to address the financial implications of cyber incidents.

In the example given, a cyber incident might trigger property damage, and this aspect could be covered under a standard property insurance policy. Recognizing such overlaps is crucial for insured organizations to avoid unnecessary expenses and ensure that they are adequately protected.

Insured organizations should conduct a comprehensive review of their current insurance policies to identify any clauses or provisions related to cyber risks. This involves looking at property insurance, general liability insurance, and any other relevant policies to determine whether they offer any level of cyber incident coverage. While assessing existing policies, it's

equally important to identify any exclusions or limitations related to cyber risks. Some policies may explicitly exclude coverage for cyber-related events, while others may have limitations that could leave gaps in protection. Understanding these aspects helps organizations make informed decisions about whether additional cyber insurance is necessary.

In summary, the insured should be proactive in understanding how their existing insurance policies may or may not cover cyber incidents. This involves a thorough review of policy terms, conditions, and exclusions. By assessing their current coverage and taking necessary steps to address potential gaps, organizations can better prepare for the financial and operational consequences of cyber incidents (ISO, 2018).

Exclusions

Cyber insurance policies are designed to protect businesses from the financial and legal consequences of cyberattacks and data breaches. However, it's important to understand that not all cyber incidents and related losses are covered by these policies. Cyber insurance policies typically come with a set of exclusions to limit their scope and manage risks. Here are some common coverages that are often excluded from a standard cyber insurance policy:

- War and Terrorism: Most cyber insurance policies exclude coverage for losses resulting from acts of war, terrorism, or acts of nation-states. Cyberattacks with a clear state-sponsored origin may fall under this exclusion.
- Intentional Acts: Cyber insurance policies typically do not cover losses resulting from intentional or criminal acts by the policyholder or employees. This includes insider threats where an employee deliberately causes a data breach.
- Bodily Injury or Property Damage: Cyber insurance policies usually do not cover physical injury or damage to tangible property. They are primarily focused on financial losses, data breaches, and the costs associated with mitigating those events.
- Intellectual Property: In the event of theft, it is crucial to assess whether the cyber insurance policy extends coverage to potential losses of intellectual property. It's important to note that cyber insurance cannot comprehensively protect against every instance of proven or alleged infringement, utilization, improper acquisition, or exposure of patents or trade secrets. Nevertheless, certain cyber insurance policies may provide coverage for violations of intellectual property rights, such as copyrights and trademarks.

- Confidential Information: It's important for the insured to be mindful that some cyber insurance plans exclude coverage for instances of theft or unintentional exposure of confidential data.
- Reputation: The potential damage to one's reputation resulting from a cyber incident is another consideration. Typically, this aspect is excluded from coverage under a cyber insurance policy.

It's crucial for policyholders to thoroughly review and understand the terms, conditions, and exclusions of their cyber insurance policy. Additionally, businesses should work closely with their insurers to customize policies to their specific needs and risks, as coverage options can vary widely between insurers and policies (ISO, 2018).

Coverage amount limits

Cyber insurance coverage amount limits are crucial aspects of a policy that determine the financial protection an organization receives in the event of a cyber incident. Cyber insurance policies often include an excess or deductible clause, representing the sum that the insured party must cover before they can initiate a claim under the cyber insurance policy. The specific amount and terms of this excess or deductible should be determined during the crafting of the cyber insurance policy.

Additionally, cyber insurance plans may incorporate a waiting period spanning several days before business disruption coverage becomes effective. Additionally, the duration of business interruption protection within a cyber insurance policy may be restricted, typically providing compensation for income losses resulting from a cyber event for a specific time frame (ISO, 2018).

Insurance Programs

Insurance providers may offer various insurance programs tailored to different types of organizations, industries, or specific cyber risk profiles.

- Small and medium-sized enterprise (SME) plans: These programs are tailored to the unique requirements and financial constraints of smaller firms, and they offer crucial coverage for typical cyber hazards.
- Programs tailored to a particular industry: Some sectors, including the financial services, healthcare, or technology, may have specialist insurance plans that handle the particular cyber threats and regulatory requirements that apply to those fields.

- Risk management services: Insurance companies could give extra services to assist businesses in properly managing and reducing cyber threats. Risk analyses, cybersecurity consultancy, staff education, and incident response preparation are a few examples of this.

It is important for organizations considering cyber insurance to carefully evaluate their specific needs, assess their risk profile, and work closely with insurance providers to tailor policies that adequately address their cyber risks. Regular reviews and updates of coverage are also necessary to ensure that the insurance remains aligned with the evolving cyber threat landscape and the organization's changing risk profile.

Chapter 3 - Analysis of leveraging cyber insurance as a complementary option for risk mitigation

3.1. Advantages of cyber insurance as a risk management tool

According to recent reports, the estimated size of the cyber insurance market is around USD 3 billion. The market's attractiveness is evident from the increasing number of insurance companies continuously introducing new products and revisiting existing ones to make them more appealing to customers. Even companies that were initially hesitant to join the cyber insurance market are now entering or planning to enter it OECD (2017).

The main reason behind this trend is the market's profitability, primarily due to the limited number of claims filed so far. Some customers purchase cyber insurance to comply with industry-specific regulations or executive board requests without necessarily intending to make a claim. However, insurers expect the profitability landscape to change in the future as the balance between policies written and claims incurred is likely to shift.

As the cyber insurance market continues to expand, competition among underwriters will increase. To secure their market share, insurance companies must gain a better understanding of their customers' needs and design policies that align with them. Insurers have already recognized the distinction between large enterprises and small to medium-sized enterprises (SMEs), as each segment has different needs and varying levels of exposure to cyber risks.

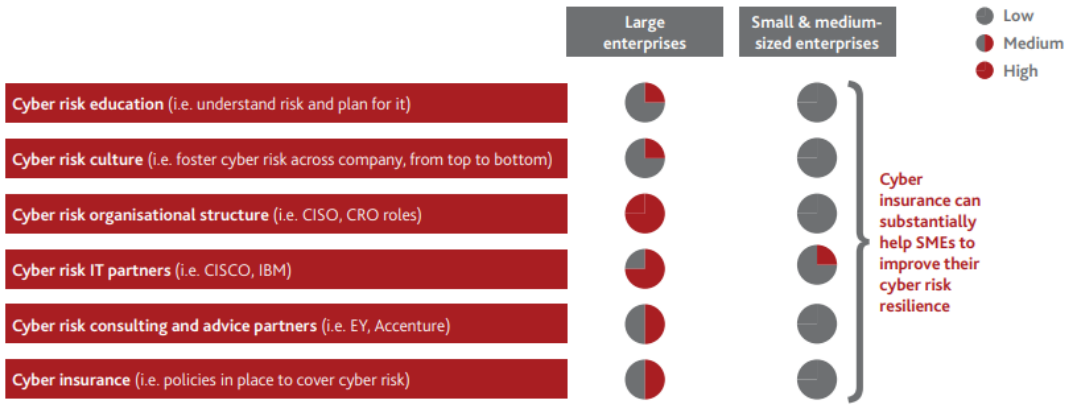


Figure 1- Cyber risk readiness by customer segment

Source: (Geneva Association, 2018)

Large enterprises, such as major financial institutions, typically have well-equipped IT departments and dedicated resources to manage cyber risks. They often have Chief Risk

Officers and Chief Information Security Officers who possess a deep understanding of their vulnerabilities and exposures. Additionally, large companies usually have cyber insurance policies and collaborate with external cyber risk consultants to mitigate their exposure. Cyber insurance market is in a state of growth and transformation. Insurance companies are adapting their offerings to cater to customers' diverse requirements, particularly distinguishing between large enterprises and SMEs. As the market matures and claims increase, insurers will face new challenges, requiring a strategic approach to maintain their competitiveness and meet the evolving demands of their customers (Geneva Association, 2018).

On the contrary, the landscape for small to medium-sized enterprises (SMEs) presents a markedly different scenario. While there may be exceptions, as a group, SMEs often lack the expertise and resources necessary to effectively address cyber risk. They are generally unaware of their vulnerabilities and risk exposures, and unlike large enterprises, they do not have dedicated teams to handle cyber risk. Even if they do have such teams, they are often too small and limited in diversity to provide adequate protection. Consequently, many SMEs outsource a significant portion of their IT and cybersecurity functions. While the cyber insurance market holds promising potential for SMEs, insurers face challenges in demonstrating the value of insurance to businesses less familiar with cyber risks. Convincing SMEs to invest their time and resources in purchasing cyber insurance can be difficult, and the returns on these efforts may not always be substantial (Geneva Association, 2018).

Sales process for cyber insurance is slow and costly. It involves creating cyber awareness among potential customers and educating them on how to assess their exposure to cyber risks. This prompts the question of how underwriters and brokers can attract more SME customers to cyber insurance.

One observed trend is the need for clear definitions of which insurance policies cover cyber risk. Currently, cyber risk coverage is either included as part of existing policies or offered as stand-alone insurance products. However, there is often confusion about which events are covered by specific policies, leading to a lack of customer awareness and understanding of available cyber insurance options. Enhancing clarity in this regard can help increase SMEs' interest in cyber insurance (Geneva Association, 2018).

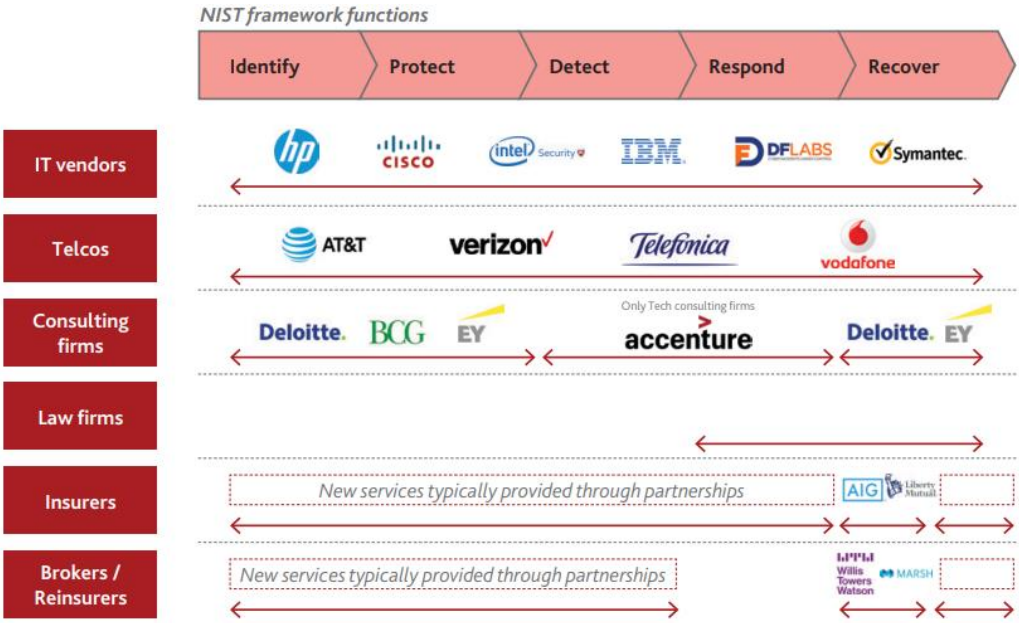


Figure 2- Cyber risk value chain (non-exhaustive)

Source: (Geneva Association, 2018).

The second trend, centers around standardizing and simplifying the language used in cyber insurance policies. Many customers who are not well-versed in cyber insurance find it challenging to comprehend the complexities of policies and premiums. Underwriters and brokers can play a crucial role in educating customers during this process.

Lastly, insurance companies are actively working to demonstrate the added value of cyber insurance to organizations beyond mere coverage. This entails showcasing how cyber insurance can provide comprehensive risk management solutions, including preventive measures, incident response, and recovery support (Geneva Association, 2018).

3.1.1. Financial Protection

Cyber insurance provides financial protection to organizations in the occur of a cyber incident. Moreover, cyber insurance help organizations to cover the costs associated with data breaches, network intrusions, ransomware attacks, and other cyber threats. This includes expenses related to incident response, forensic investigations, legal fees, regulatory fines, and potential lawsuits. By transferring the financial risk to an insurance provider, organizations can mitigate the financial impact of cyber incidents and ensure business continuity.

3.1.2. Risk Transfer

Cyber insurance enables organizations to transfer a portion of their cyber risk to an insurance carrier. Cyber insurance is an emerging market that is rapidly evolving. Insurance

companies are still in the process of entering and familiarizing themselves with the market, while customers may remain skeptical or uncertain about its potential. However, there is a consensus that the market will experience significant growth in the coming years (Tondel et al., 2019).

This transfer of risk helps mitigate the potential financial losses and liabilities associated with cyber incidents. Instead of bearing the full cost of recovery and compensation themselves, organizations can share the risk with the insurance provider, reducing their exposure to financial and operational risks.

3.1.3. Enhanced Incident Response

Many cyber insurance policies include access to incident response services. This can involve immediate assistance from experts in cybersecurity, forensic investigations, and breach notification procedures. The availability of these services helps organizations respond effectively to cyber incidents, minimize the impact of the breach, and facilitate timely recovery (Smeenk, 2017).

3.1.4. Risk Assessment and Improvement

During the underwriting process, cyber insurance carriers often conduct risk assessments of the insured organization's cybersecurity practices. This evaluation can provide valuable insights into existing vulnerabilities and weaknesses in the organization's security posture. Organizations can use this information to identify areas for improvement, strengthen their cybersecurity measures, and enhance their overall risk management approach (Smeenk, 2017).

Requirements for Compliance and Risk Management

Organizations are frequently required by cyber insurance plans to follow particular security and risk management procedures. If these conditions are not met, coverage may be restricted or excluded. To comply with the policy's compliance and risk management requirements, organizations must make sure they have the proper cybersecurity controls and risk management frameworks in place.

Possibility of Moral Hazard

A moral hazard might result from the existence of cyber insurance, wherein covered firms may be less driven to invest in effective cybersecurity solutions or effectively manage their cyber risks. To prevent complacency and maintain a proactive cybersecurity posture, it is crucial for enterprises to find a balance between depending on insurance coverage and putting into place effective risk management procedures (Dioubate et al., 2022).

By examining the advantages and limitations of cyber insurance as a risk management tool, organizations can gain a comprehensive understanding of how this approach fits within their overall cybersecurity strategy. This analysis sets the foundation for further exploration into the effectiveness and suitability of cyber insurance as a complementary option for mitigating cyber risks in modern business and organizational environments.

3.2. Cyber insurance services/coverage and strategies

Cyber insurance has gained significant attention in recent years within the research and insurance industries. It encompasses a broad array of perspectives, including information technology, economic, statistical, and actuarial viewpoints. The increasing proliferation of interconnected devices and global internet availability has led to the emergence of cyber insurance as a dynamic and evolving business sector for the insurance industry. Policyholders seek to mitigate financial losses resulting from cyber-attacks by transferring cyber risks to a third party through acquiring cyber insurance. This compensation is typically provided collectively and over a specified period. Unlike conventional insurance products, cyber insurance goes beyond mere financial compensation and offers a range of services aimed at minimizing adverse impacts on organizations from cyber incidents. In exchange for a premium payment, insurers commit to providing loss-dependent benefits in the event of contractually agreed loss events (Tondel et al., 2019).

Cyber insurance policies cover "first-party" losses incurred by the policyholder and "third-party" losses caused by the policyholder to external parties outside the policy. However, despite the formal existence of cyber insurance, its current coverage appears inadequate in the face of the escalating cyber risks. The surge in cyber-attacks has also fueled the scientific community's interest in cyber insurance, evident from the abundance of related publications. Different terms are used to refer to cyber insurance policies, including "cyber risk insurance," "cyber liability insurance," "data breach liability insurance," "internet insurance," and "cyber security insurance," all of which are commonly used interchangeably (Meland et al., 2018).

The insurance market offers three distinct categories of cyber coverage:

a. standalone cyber policies,

b. cyber coverage integrated into existing traditional insurance products,

c. silent cyber coverage, which refers to policies without explicit exclusions or gaps.

Regulatory authorities, such as those in Germany and the EU, are increasingly considering the issue of silent cyber coverage (Peters et al., 2017). With the growing frequency

of cyber incidents and increased awareness of cyber risks, industry experts anticipate a rise in demand for cyber insurance policies.

While previous studies have primarily focused on companies as customers of cyber insurance, the market is also expected to expand to include consumers. As the Internet of Things (IoT) gains significance and digital resource usage carries higher risk exposure, both companies and consumers are becoming potential targets for cyber insurance coverage. Existing studies have explored the cyber insurance ecosystem, but they often neglect consumers as actors, focusing mainly on companies as policyholders. Although specialized insurance products such as Identity Theft Insurance exist for consumers, they only cover a subset of potential cyber losses. Therefore, a more comprehensive investigation of various insurance lines available to consumers, including Identity Theft Insurance, seems relevant (Meland et al., 2018).

In conclusion, consumer cyber insurance represents a specific risk transfer option for private households and serves as an essential focus of our study. By explicitly examining consumers as policyholders of available cyber insurance product lines, we aim to contribute to the understanding and analysis of cyber insurance in the broader context of risk management strategies.

3.2.1. Insurance services

Cyber Insurance companies offer various services and coverage to protect against cyber-attacks and their consequences. Depending on the type of insurance and contracts, services provided may vary, but some common features include:

Compensation and Restoration

In the event that a company is the victim of a cyber-attack and suffers damages, Cyber Insurance can cover financial losses, legal costs and system restoration costs. In today's digital era, businesses face a multitude of cyber risks, including data breaches, malware infections, and denial-of-service attacks, which can lead to substantial financial losses and legal liabilities. In such unfortunate circumstances, Cyber Insurance assumes a vital role in providing compensation and restoration services to companies that fall victim to cyber-attacks. By offering financial support, Cyber Insurance helps alleviate the burden imposed by these incidents and aids businesses in their recovery efforts (Bodin et al., 2018).

Compensation forms a fundamental aspect of Cyber Insurance, entailing the reimbursement of the insured company for the financial losses incurred due to the cyber-attack. This includes both direct costs associated with incident response and recovery, as well as indirect expenses stemming from business interruptions and revenue losses. By shouldering

these financial burdens, Cyber Insurance empowers businesses to swiftly recuperate and sustain their operations without enduring severe financial setbacks (Bodin et al., 2018).

Additionally, cyber-attacks often involve complex legal implications, exposing companies to potential litigation or regulatory fines. In such scenarios, legal costs can rapidly escalate, posing significant challenges for businesses (Cyber Insurance Market Conditions Report, 2021). Here, Cyber Insurance proves valuable, as it extends coverage for legal fees and settlement expenses. This financial backing provides businesses with the confidence to navigate intricate legal landscapes, including compliance with data protection laws, and minimize their vulnerability to costly legal disputes.

Moreover, a critical aspect of Cyber Insurance is its coverage for system restoration costs. Following a cyber-attack, businesses must undertake the arduous task of repairing and restoring their compromised systems and networks. This process can be both time-consuming and expensive, particularly if vital data has been compromised. Cyber Insurance intervenes to shoulder the financial burden of system restoration, allowing businesses to swiftly regain functionality and resume normal operations (peters et al., 2017).

In essence, the compensation and restoration services rendered by Cyber Insurance play an indispensable role in safeguarding businesses against cyber threats. By providing financial support for losses, legal expenses, and system restoration, Cyber Insurance offers businesses peace of mind and enables them to focus on their core activities without undue worry about the financial repercussions of a cyber-attack. By encouraging proactive cybersecurity measures and fostering resilience in the face of ever-evolving cyber risks, Cyber Insurance has become an integral component of comprehensive risk management strategies for businesses in today's digital landscape (Bodin et al., 2018).

Data Protection

Cyber Insurance companies offer cover for leakage or theft of sensitive data such as personal customer information or confidential business information. With businesses increasingly dependent on technology and the internet, the risk of data breaches has become more pronounced, posing a significant threat to customer information and proprietary data. The consequences of such breaches are far-reaching, encompassing not only financial losses but also potential damage to a company's reputation and erosion of customer trust. In response to these pressing threats, Cyber Insurance companies step in to provide essential coverage, offering a safeguard to businesses against the potentially devastating impacts of data breaches (Cyber Insurance Market Conditions Report, 2021).

The coverage provided by Cyber Insurance companies for data breaches spans a wide array of scenarios. Whether it involves a deliberate cyber-attack orchestrated by sophisticated hackers or accidental data exposure due to employee errors, the aftermath of such incidents can

be substantial. Cyber Insurance not only assists in compensating for financial losses resulting from these events but also facilitates the implementation of effective risk mitigation strategies. By securing appropriate coverage, businesses can proactively work towards preventing similar breaches in the future and ensure robust protection for sensitive data (Ponemon, 2019).

Moreover, the significance of safeguarding personal customer information cannot be overstated. In an era characterized by heightened data privacy concerns and stringent regulatory requirements, businesses face mounting pressure to protect the personal data they handle. The failure to do so can lead to severe penalties and legal repercussions. Cyber Insurance companies offer tailored solutions that cater to the specific data protection needs of businesses, providing invaluable assistance in adhering to relevant data protection laws and regulations.

Beyond the realm of customer data, businesses often possess critical and confidential information vital to their operations and competitiveness. This may encompass proprietary research, trade secrets, and strategic plans. A data breach that exposes or results in the theft of such sensitive business information can significantly undermine a company's competitive advantage and market position. Acknowledging the value of such data, Cyber Insurance companies extend coverage to safeguard against its compromise or unauthorized access.

Cyber Insurance companies act as indispensable guardians, providing comprehensive coverage for the risks associated with the leakage or theft of sensitive data in an increasingly interconnected world. By offering financial protection and tailored risk management solutions, they empower businesses to navigate the intricate challenges posed by data breaches and cyber threats with efficacy (Howden, 2021).

The importance of such coverage cannot be emphasized enough, as it not only protects financial interests but also reinforces a company's resilience, reputation, and overall cybersecurity posture within the ever-evolving landscape of data security challenges. Given the escalating reliance on digital technologies, the role of Cyber Insurance in safeguarding sensitive data will undoubtedly remain paramount for businesses across various industries and scales.

Systems security

Insurance companies may provide coverage for losses resulting from malware and other forms of cyber-attacks that can lead to disruption of digital services. As technology advances at a rapid pace, cyber threats have also become more sophisticated and pervasive, posing substantial risks to the confidentiality and integrity of sensitive data. Recognizing the escalating nature of these risks, insurance companies have acknowledged their vital role in offering coverage for losses resulting from cyber-attacks, particularly those that exploit malware and other malicious methods to disrupt digital services (Howden, 2021).

Malware, encompassing viruses, ransomware, and trojans, stand as a major threat to the security of digital systems. These malicious software programs infiltrate and compromise a company's network, leading to dreadful consequences such as data breaches, business interruptions, and financial losses. In response to this concerning trend, Cyber Insurance policies have evolved to address these specific risks, providing coverage for the financial impact caused by malware attacks (Balawejder, 2019).

A primary advantage of Cyber Insurance lies in its ability to offer financial compensation to aid businesses in recovering from the financial losses incurred due to cyber-attacks. This includes covering costs related to identifying and mitigating the effects of malware, involving services of cybersecurity experts, conducting forensic investigations, and implementing measures for remediation. Additionally, Cyber Insurance extends to cover expenses associated with business interruption, as systems may require temporary shutdowns to contain the malware and ensure thorough cleanup.

Insurance companies also acknowledge the importance of prevention and mitigation when it comes to the enduring impacts of cyber-attacks on digital services. For this reason, Cyber Insurance policies may incorporate risk management services with a focus on enhancing systems security. By collaborating with cybersecurity experts, insurers provide proactive guidance, training, and best practices to bolster the overall security posture of organizations. This approach not only benefits the insured businesses but also aligns with the insurer's interest in reducing the likelihood and severity of future cyber incidents.

In addition to safeguarding against malware attacks, Cyber Insurance offers coverage for an array of cyber threats that threaten systems security. These may include denial-of-service (DoS) attacks that overload and disrupt online services, phishing attacks exploiting human vulnerabilities for unauthorized access, and insider threats arising from employees or contractors with malicious intent. By encompassing such diverse cyber risks, insurance companies assist businesses in navigating the intricate complexities of the digital landscape and fostering resilience against ever-evolving threats (Balawejder, 2019).

Security of digital systems represents a pressing concern for businesses in the face of the escalating frequency of cyber-attacks. Cyber Insurance has emerged as an priceless tool to protect against the financial repercussions of malware and other cyber threats disrupting digital services (Balawejder, 2019).

By providing compensation for losses and collaborating with cybersecurity experts to enhance risk management practices, insurance companies make a significant contribution to fortifying the cybersecurity posture of organizations. As technology continues to advance, Cyber Insurance will undoubtedly retain its pivotal role as a fundamental component of comprehensive risk management strategies, essential for safeguarding systems and sensitive information in the digital realm.

Coverage of DDoS attacks

DDoS attacks can cause service interruptions due to overloading of network infrastructures. Cyber Insurance can provide coverage for damages resulting from these attacks. DDoS (Distributed Denial of Service) attacks pose a significant and grave threat to the security of digital services and networks. These malicious attacks involve the coordinated efforts of malevolent users or botnets, directing an overwhelming volume of illicit traffic towards specific targets. This flood of traffic overloads network infrastructures, effectively blocking legitimate users from accessing the services they rely on (Boran et al., 2022).

The impact of DDoS attacks on businesses can be severe. The resulting downtime translates to lost revenue, decreased productivity, and limited room for effective response strategies. Moreover, the aggressive nature of DDoS attacks can inflict damage to a company's reputation, eroding customer confidence and negatively influencing its business environment (Boran et al., 2022).

To address the repercussions of DDoS attacks, Cyber Insurance emerges as an effective solution. By offering appropriate insurance policies, companies gain coverage against the damages arising from such attacks, thus enabling compensation for corresponding monetary losses. This encompasses the expenses associated with technical efforts to combat the attack, restore services, and offset any revenue loss stemming from the service disruption.

Beyond financial compensation, Cyber Insurance goes a step further by providing proactive services to safeguard against future DDoS attacks. Collaborating with cybersecurity experts, insurance companies provide valuable guidance and training to establish and implement robust security best practices. This proactive approach bolsters organizations' resilience against ever-evolving threats and elevates their overall security posture.

Overall, coverage for DDoS attacks through Cyber Insurance is not only essential but also robust, providing a necessary layer of insurance protection. It equips businesses to cope with the unpredictable and detrimental consequences of DDoS attacks, offering critical support for restoring functionality and safeguarding digital assets. As technology advances, Cyber Insurance will continue to play a vital role in preserving the safety and well-being of organizations in the dynamic landscape of the digital world.

3.2.2. Risk assessment

Cyber Insurance and the protective services of cyber security companies are a comprehensive approach to data security and protection against cyber-attacks. With the

continuous development of technology and the increase in cyber threats, the importance of cyber security and Cyber Insurance is expected to increase further.

When it comes to how data is protected, Cyber Insurance companies usually seek to improve the cybersecurity of their clients. This can be achieved through:

- Risk assessment: Companies carry out an assessment of the cyber threats faced by each client and propose appropriate solutions.
- Training: They provide training to their clients' employees to identify and deal with cyber threats.
- Security services: They offer cyber security services, such as firewall, antivirus, intrusion detection systems, etc., to protect their customers' networks and systems.
- Crisis Communication: Provide services to respond to and recover from the consequences of a cyber-attack, including crisis communication and crisis management.

Cyber Insurance providers play a crucial role in delivering essential risk assessment services, which constitute a pivotal step in evaluating and responding to cyber threats. Risk assessment involves the systematic process of identifying, analyzing, and evaluating potential risks that an organization may encounter in the digital realm.

Collaborating with cybersecurity experts, Cyber Insurance companies actively pinpoint the specific cyber risks that a business may confront. This comprehensive approach encompasses the identification of potential cyber threats, assessment of security system weaknesses, and scrutiny of vulnerabilities within the company's network and applications.

Leveraging the insights gained from risk assessment, Cyber Insurance companies offer personalized and tailored insurance plans. This means that the insurance policies are designed to cater to the distinct needs and susceptibilities of each individual business. By providing customized solutions, Cyber Insurance companies ensure that enterprises are shielded from the precise cyber risks that could potentially jeopardize their operations.

Moreover, the risk assessment process remains an ongoing aspect throughout the insurance coverage period. Cyber Insurance companies maintain consistent communication with their clients and diligently monitor the evolving landscape of cyber risks. This vigilant approach allows them to adapt and fine-tune insurance solutions to effectively address any emerging threats that may arise during the coverage period. Cyber Insurance companies offer risk assessment services, empowering businesses to comprehend and proactively combat the cyber threats they encounter. Through personalized insurance solutions and continuous

monitoring, these companies contribute significantly to safeguarding enterprises against cyber risks and fostering a competitive and secure presence in the ever-evolving digital world.

3.3. Practical application examples and case studies

Over the past years, the cyber insurance sector has experienced substantial growth, primarily due to the escalating frequency of cyber-attacks and the critical need to safeguard both personal and corporate data. The relative lack of legal precedent on crucial issues related to cyberattacks adds to the uncertainties faced by insurers as they navigate this emerging market. When grappling with uncertainty over fundamental questions, insurers may adopt a cautious approach, choosing to wait until these issues are resolved before offering policies, or they might write policies with restrictive coverage, which may be less beneficial to businesses seeking comprehensive protection. For instance, data breaches and data theft are common sources of damages from cyberattacks, but there is still unresolved legal ambiguity surrounding these cases. Legal disputes concerning data breaches often revolve around the nature of the harm suffered by the individuals whose data was exposed. Some courts have ruled that victims of data breaches lack standing to sue unless actual identity theft or fraud has occurred, while others have granted standing based on the risk of data misuse resulting from the breach (Kesan, Jay & Hayes, Carol, 2017).

The Supreme Court has not directly addressed the issue of standing in data breach litigation, leading to ongoing uncertainty. This lack of clarity on standing in data breach litigation holds significant implications for cyber insurers, as it directly impacts the likelihood that an insurer may have to pay claims in the event of a data breach. Consequently, it affects how insurers should price their insurance policies. Additionally, lawsuits directly related to cyber insurance coverage have already emerged.

An illustrative case that holds significant implications for the cyber insurance market involved a dispute between Mondelēz International and Zurich Insurance Group. This dispute arose over the interpretation of a common "act of war" exclusion in the insurance contract. Mondelēz claimed $100 million in damages resulting from the “NotPetya” cyberattack, but Zurich denied the claim, asserting that the attack qualified as an "act of war." The case highlights the need for specific language in cyber insurance policies to address the nature of both the crime and the perpetrator, thus avoiding legal conflicts.

Another source of uncertainty stems from an untested feature of cyber insurance law, namely, the 2002 Terrorism Risk Insurance Act (TRIA). Enacted after the 9/11 terrorist attacks, TRIA mandates property and casualty (P&C) insurers to offer terrorism risk insurance and specifies that the U.S. government will cover damages caused by certified acts of terrorism

exceeding a predetermined threshold. How this law applies to cyber incidents is yet to be tested, and its potential impact on cyber insurance claims remains uncertain. In conclusion, the evolving landscape of cyber insurance is accompanied by legal complexities and uncertainties, requiring insurers to carefully assess and adapt their policies to address emerging cyber risks adequately. The resolution of legal ambiguities and the establishment of clear precedents will play a pivotal role in shaping the future of the cyber insurance market and its effectiveness in providing comprehensive coverage to businesses in the face of cyber threats (Drexler et al., 2020).

The emerging cyber insurance market faces significant uncertainties due to the lack of well-established legal precedents on crucial issues related to cyberattacks. Insurers navigating this landscape often adopt a cautious approach, either waiting for resolution on fundamental questions or providing policies with restrictive coverage, potentially limiting the comprehensive protection sought by businesses. Notably, data breaches and data theft, common sources of cyberattack damages, are still surrounded by legal ambiguity. Litigations concerning data breaches revolve around the harm suffered by individuals whose data was exposed, leading to inconsistent court rulings on standing to sue. Some courts require actual identity theft or fraud to grant standing, while others recognize the risk of data misuse resulting from breaches.

In conclusion, the cyber insurance market's evolving nature is accompanied by legal complexities and uncertainties. Insurers must carefully evaluate and adjust their policies to effectively address emerging cyber risks. The resolution of legal ambiguities and the establishment of clear precedents will significantly influence the future of the cyber insurance market, ensuring its ability to provide comprehensive coverage to businesses facing cyber threats (Granato, 2019).

As of September 2021, several prominent cyber insurance companies were known for their robust presence in the market. The following section presents some basic data about these cyber insurance companies

3.4. Most known Cyber insurance Companies

Chubb Limited

Chubb is a globally recognized insurance company that specializes in providing coverage for cyber threats and a wide range of cyber-attacks. Chubb Limited: As a globally recognized insurance company, Chubb stands at the forefront of the cyber insurance industry, offering specialized coverage to address the ever-evolving landscape of cyber threats. With a reputation built on reliability and innovation, Chubb has become a trusted partner for businesses seeking robust protection against a wide range of cyber-attacks.

Understanding the dynamic nature of cyber risks, Chubb takes a comprehensive approach to cyber insurance, tailoring its offerings to meet the unique needs of each client. Their expert team of underwriters collaborates closely with cybersecurity specialists to conduct thorough risk assessments, identifying potential vulnerabilities and devising effective risk management strategies.

Chubb's cyber insurance policies go beyond the conventional scope of coverage, extending to address emerging threats such as ransomware attacks, data breaches, and business email compromise. By providing financial protection against these sophisticated threats, Chubb empowers businesses to navigate the digital landscape with confidence, knowing they have a reliable safety net in place.

Moreover, Chubb's commitment to its clients extends beyond just financial compensation. The company takes a proactive approach to risk mitigation, offering guidance and support to enhance the cybersecurity posture of its policyholders. Through educational resources, best practices, and incident response assistance, Chubb equips businesses with the knowledge and tools to fortify their defenses against cyber adversaries.

With a global presence, Chubb is equipped to serve businesses across various industries and geographical regions. Whether it's a multinational corporation or a small-to-medium-sized enterprise, Chubb's cyber insurance solutions are designed to adapt to the unique challenges faced by each client.

Through a combination of cutting-edge technology, extensive industry knowledge, and a client-centric approach, Chubb has solidified its position as a leading cyber insurance provider. Businesses looking to safeguard their digital assets, customer data, and reputation can rely on Chubb's expertise and unwavering commitment to mitigating cyber risks. As the cyber threat landscape continues to evolve, Chubb remains at the forefront of innovation, continually refining its offerings to provide the most effective and up-to-date cyber insurance coverage.

AIG (American International Group)

AIG is a leading provider of insurance services, offering cyber insurance to shield against various cyber-attacks. Renowned as a leading provider of insurance services, AIG has solidified its position in the cyber insurance market by offering comprehensive coverage to shield businesses against the ever-expanding array of cyber-attacks. With a rich history and global reach, AIG has become synonymous with reliability and expertise in navigating complex risks, making it a preferred choice for businesses seeking robust cyber insurance solutions (Herath, 2019).

Recognizing the magnitude of cyber threats and their potential to disrupt businesses of all sizes, AIG has developed a diverse portfolio of cyber insurance policies tailored to address

the unique needs and vulnerabilities of different industries. From multinational corporations to startups, AIG's cyber insurance offerings cater to a broad spectrum of clients, providing them with the necessary tools to safeguard their digital assets and sensitive information (Herath, 2019).

One of AIG's core strengths lies in its proactive approach to risk assessment and management. The company collaborates with cybersecurity experts and data analysts to conduct in-depth evaluations of potential cyber risks faced by its clients. By identifying weak points and potential entry points for cyber attackers, AIG empowers businesses to fortify their defenses and reduce their susceptibility to cyber incidents.

AIG's cyber insurance coverage extends far beyond financial compensation for losses incurred from cyber-attacks. The company recognizes the importance of swift incident response and recovery, and as such, offers 24/7 support to assist policyholders in managing and mitigating the impact of cyber incidents. This includes access to experienced incident response teams, forensic experts, and legal counsel to help navigate the complexities of cyber breaches.

Furthermore, AIG's commitment to education and risk awareness sets it apart in the cyber insurance landscape. The company provides clients with valuable resources, such as cybersecurity training programs and best practices, empowering them to foster a culture of cyber resilience within their organizations. AIG's focus on proactive risk management aligns with its dedication to helping clients minimize cyber threats before they escalate into costly and damaging breaches.

AIG's global presence and extensive network of partners enable the company to offer seamless cyber insurance solutions to businesses operating in various regions around the world. Whether it's protection against data breaches, ransomware attacks, or other cyber perils, AIG's cyber insurance coverage can be tailored to fit the specific needs of each client, regardless of their industry or size.

In an age where cyber risks continue to evolve and escalate, AIG remains at the forefront of innovation, continuously adapting its cyber insurance offerings to address emerging threats and challenges. Businesses entrust AIG to be their strategic ally in the fight against cyber adversaries, knowing they have a reliable partner that shares their commitment to safeguarding digital assets and maintaining business continuity in an interconnected world.

Allianz

As a powerhouse multinational insurance company with a long-standing legacy of excellence, Allianz takes a forward-looking approach to address the evolving landscape of cyber risks. Recognizing the profound impact of cyber threats on businesses of all scales, Allianz has strategically expanded its insurance offerings to encompass comprehensive cyber

insurance, providing clients with robust protection against a wide array of cyber risks (Allianz Global Corporate & Specialty, 2017).

With a global presence and a vast network of experts, Allianz is uniquely positioned to serve clients across diverse industries and geographic regions. From small businesses to large corporations, Allianz's cyber insurance solutions cater to the specific needs and vulnerabilities of each client, ensuring they have the necessary tools to defend against cyber adversaries.

Allianz's commitment to proactive risk management is evident in its rigorous risk assessment process. The company collaborates with cybersecurity specialists and data analysts to conduct thorough evaluations of potential cyber risks faced by its clients. By identifying vulnerabilities and potential points of entry for cyber attackers, Allianz empowers businesses to bolster their cyber defenses and minimize their exposure to cyber incidents.

Beyond financial compensation for losses, Allianz goes the extra mile to offer valuable services that help clients navigate the complexities of cyber incidents. The company's proactive approach includes providing access to experienced incident response teams, cyber forensic experts, and legal counsel, all of which are crucial resources for efficiently managing and mitigating the impact of cyber breaches (Allianz Global Corporate & Specialty, 2017).

One of Allianz's strengths lies in its customer-centric approach. The company strives to build strong partnerships with its clients, engaging in open and transparent communication to understand their unique cyber risk profiles. By tailoring cyber insurance coverage to match the specific requirements of each client, Allianz ensures that businesses receive the most relevant and effective protection against cyber threats.

Moreover, Allianz recognizes the importance of fostering a cyber-aware culture within organizations. As part of its comprehensive cyber insurance offerings, Allianz provides educational resources and cybersecurity training programs to its clients, helping them enhance their internal cybersecurity practices and promote a proactive risk management mindset.

Allianz's reputation for reliability and stability has earned it the trust of businesses worldwide. The company's robust financial strength and extensive experience in handling complex risks instill confidence in its clients, assuring them that Allianz is a dependable partner capable of safeguarding their digital assets and reputation.

As the cyber threat landscape continues to evolve, Allianz remains at the forefront of innovation, continuously refining its cyber insurance offerings to address emerging risks and challenges. By partnering with Allianz, businesses gain more than just insurance coverage; they gain a strategic ally dedicated to proactively protecting their interests in the digital realm. In an interconnected world where cyber risks are ever-present, Allianz stands tall as a beacon of security and resilience for its clients, helping them navigate the uncertainties of the cyber landscape with confidence and peace of mind.

Zurich Insurance Group

As a globally recognized insurance powerhouse, Zurich Insurance Group has been a key player in the insurance industry for over a century. With a strong commitment to innovation and adaptability, Zurich has continually evolved its offerings to meet the changing needs of businesses and individuals alike. Embracing the digital era, Zurich Insurance Group has established itself as a leader in the cyber insurance market, providing cutting-edge solutions to protect clients from the ever-growing and sophisticated cyber threats (Ferland et al., 2019).

Zurich's cyber insurance coverage is designed to address the unique challenges posed by the rapidly evolving cyber landscape. The company's expert team of underwriters and risk assessors work closely with clients to gain a comprehensive understanding of their cybersecurity posture. This collaborative approach enables Zurich to tailor cyber insurance solutions that precisely align with each client's risk profile, ensuring that businesses of all sizes receive customized protection against cyber risks (Ferland et al., 2019).

Cyber threats, such as data breaches, ransomware attacks, and business email compromise, can have devastating consequences for organizations. Zurich Insurance Group recognizes the significance of swift incident response in mitigating these impacts. Therefore, in addition to providing financial compensation for losses, Zurich offers a range of support services to assist clients in managing and recovering from cyber incidents. From 24/7 incident response teams to legal counsel and forensic experts, Zurich stands ready to help clients navigate the complexities of cyber breaches with efficiency and resilience.

Furthermore, Zurich Insurance Group goes beyond financial compensation by placing a strong emphasis on risk prevention and mitigation. The company actively promotes cyber risk awareness and provides clients with valuable resources and educational materials to enhance their cybersecurity practices. Zurich's dedication to proactive risk management empowers businesses to adopt a proactive stance against cyber threats, ultimately fostering a more cyber-resilient organizational culture.

As a multinational insurance provider, Zurich's global presence enables it to serve clients across diverse industries and geographical regions. Whether it's a small local business or a multinational corporation, Zurich's cyber insurance solutions are designed to adapt to the unique needs and challenges faced by each client. Zurich's commitment to ethical business practices, transparency, and customer-centricity has earned it a strong reputation in the insurance market. Clients trust Zurich Insurance Group to be their strategic partner in safeguarding their digital assets and reputation from cyber risks (Ferland et al., 2019).

AXA

AXA, an international insurance company, also offers specialized cyber insurance services to address the evolving cyber landscape. With a global presence and a strong reputation

in the insurance industry, AXA has been a trusted name for insurance services for many decades. Recognizing the critical importance of cyber insurance in today's digital era, AXA has expanded its offerings to include specialized cyber insurance services, catering to the unique needs and challenges posed by the ever-evolving cyber landscape (Noussia et al., 2021).

As a multinational insurance company, AXA understands the diverse cyber risks faced by businesses and individuals across different industries and geographic regions. AXA's expert team of underwriters and risk assessors collaborates closely with clients to conduct comprehensive risk evaluations, identifying potential vulnerabilities and areas of concern within their cybersecurity practices. This hands-on approach enables AXA to craft tailored cyber insurance solutions that address the specific cyber risks faced by each client, providing them with the right level of protection and peace of mind.

One of AXA's key strengths lies in its commitment to proactive risk management. In addition to offering financial compensation for losses resulting from cyber incidents, AXA places significant emphasis on prevention and mitigation. The company provides valuable resources and guidance to its clients, including cybersecurity training and best practices, empowering them to enhance their cyber defenses and minimize the likelihood of cyber-attacks (Noussia et al., 2021).

AXA's cyber insurance coverage extends to a wide range of cyber perils, encompassing data breaches, ransomware attacks, network disruptions, and other emerging cyber threats. By offering comprehensive coverage against these ever-present risks, AXA enables businesses and individuals to navigate the digital landscape with confidence, knowing they have a reliable safety net to fall back on in the event of a cyber incident.

Moreover, AXA's commitment to customer-centricity sets it apart in the cyber insurance market. The company places a strong emphasis on building long-term relationships with its clients, fostering open and transparent communication. By understanding their clients' specific needs and requirements, AXA ensures that its cyber insurance solutions align with their risk profiles, offering a tailored approach that instills confidence and trust.

As a forward-thinking insurance provider, AXA continuously adapts its cyber insurance offerings to stay ahead of emerging cyber threats. The company stays abreast of the rapidly changing cyber landscape, refining its policies and coverage options to address new and sophisticated cyber risks that emerge over time. AXA's global reach, customer-centric approach, and commitment to proactive risk management make it a formidable player in the cyber insurance domain. With AXA's specialized cyber insurance services, businesses and individuals alike can navigate the digital landscape with confidence, knowing they have a reliable partner to protect their digital assets and reputation from cyber risks. In an interconnected world where cyber threats are constantly evolving, AXA stands ready to help

clients face the challenges of the digital age and build resilience in the face of cyber adversaries (Noussia et al., 2021).

Chapter 4 - Information and data sharing between insured parties and insurance companies

In the sector of cyber insurance, the exchange of information between insured parties and insurance companies holds utmost significance. This chapter delves deep into the critical examination of the types of information that play a pivotal role in risk assessment and the determination of appropriate insurance coverage. By comprehending the specific data elements that form the foundation of this process, both parties can make well-informed decisions that align with their respective needs and objectives.

This vital information empowers insurers to evaluate the organization's vulnerability to potential cyber threats and gauge the likelihood of a cybersecurity incident occurring. Armed with a comprehensive understanding of the insured party's cybersecurity practices, insurance companies can tailor their coverage offerings to effectively address specific risks (OECD, 2020).

Moreover, the types of information needed for risk assessment go beyond the organization's internal cybersecurity measures. Insured parties often must divulge their historical experience with cyber incidents, such as past data breaches or cyber-attacks. This historical data provides valuable insights into the organization's risk exposure and assists insurers in estimating potential financial losses in the event of future cyber incidents.

Apart from the data provided by the insured party, insurance companies also gather external information to enhance risk assessment capabilities. This involves staying well-informed about industry-specific cyber threats, emerging trends in cyber-attacks, and the general cyber threat landscape. Continuous monitoring of external information sources allows insurance companies to refine their risk models and ensure that their coverage offerings remain current and relevant.

Concerning insurance coverage, the types of information shared are multifaceted. Insured parties are required to disclose specific details about the coverage they seek, including the desired extent of financial protection and any particular clauses or endorsements required. In turn, insurance companies effectively communicate the details of the policy terms, conditions, and exclusions to ensure transparency and clear understanding between both parties.

Information and data sharing within the domain of cyber insurance must strike a delicate balance. While insurance companies require comprehensive data for accurate risk assessment, insured parties must place trust in the secure and responsible handling of sensitive information. As cyber threats continue to evolve, the effectiveness of risk assessment and coverage determination relies on mutual cooperation and transparency between insured parties and insurance companies. By fostering a collaborative approach to information sharing, both

parties can proactively mitigate cyber risks and ensure comprehensive and tailored cyber insurance solutions, offering protection and peace of mind in today's digitally connected world.

4.1. Analysis of the types of information required for risk assessment and insurance coverage

4.1.1. Cyber risk Assessment (Inherent Risk)

When assessing the inherent risk exposure of the insured, insurance providers typically consider various key factors such as (ISO, 2018):

- **Industry Sector:** Different industries have varying levels of inherent risk when it comes to cybersecurity. For example, the financial sector and healthcare industry often handle highly sensitive financial and personal data, making them attractive targets for cyberattacks. Insurers assess the industry in which the insured operates to understand the unique risks associated with that sector.
- **Size of Organization:** The size of an organization can impact its risk exposure. Larger organizations often have more complex IT environments, larger volumes of data, and a higher number of endpoints (such as devices and computers). These factors can increase the potential attack surface and, consequently, the inherent risk.
- **Business Activities:** The nature of an organization's business activities plays a significant role in risk assessment. Some activities involve higher levels of online transactions, data processing, or interactions with third parties, which can introduce additional cybersecurity risks.
- **Extent and Type of Information:** The volume and type of information an organization stores and uses are crucial factors. Highly sensitive data, such as customer financial records or healthcare records, increases the attractiveness of an organization as a target. Insurers assess the nature and quantity of data to determine risk exposure.
- **Dependency on Externally Managed or Outsourced Systems:** Organizations that rely heavily on external vendors, cloud services, or outsourced systems may

face increased risk due to factors beyond their direct control. These dependencies can introduce vulnerabilities if not managed properly.

- **Countries of Business Activities:** The geographic spread of an organization's operations can affect risk exposure. Operating in regions with a higher prevalence of cyber threats or inadequate cybersecurity regulations can increase inherent risk. Insurers consider the global footprint of the insured's business.
- **Regulatory Environment:** The regulatory landscape plays a crucial role in determining risk. Organizations subject to strict data protection and cybersecurity regulations face legal and financial consequences for non-compliance. Insurers evaluate whether the insured is subject to such regulations and assess their compliance posture.
- **Historical Cyber Incidents:** An organization's past experiences with cybersecurity incidents and breaches can also impact risk assessment. A history of significant breaches may indicate vulnerabilities or weaknesses that need attention.

4.1.2. Security controls Assessment (Residual Risk)

To commence the process of security controls Assessment of the insured requires a comprehensive collection of information from the insured parties. Insurance companies heavily rely on detailed insights into the insured entity's cybersecurity posture, encompassing aspects such as (ISO, 2018).:

- **Information Security Policies:** Information security policies provide a clear and unequivocal direction for the insured organization regarding how information security should be approached. They establish the organization's stance on safeguarding sensitive data, systems, and networks. This clarity ensures that all employees and stakeholders understand the importance of information security and the organization's commitment to it. These policies align information security efforts with the organization's broader objectives. They ensure that security measures are not seen as obstacles but as enablers of the organization's mission. By clarifying the link between security and business goals, policies help avoid conflicts and resistance to security practices.

- **Organization of Information Security:** Organization of information security is to establish role clarity. By clearly defining who is responsible for what aspects of information security, it eliminates ambiguity and ensures that everyone understands their role in safeguarding sensitive data and systems. Clear roles and responsibilities help prevent conflicts of interest. When individuals have well-defined roles, they are less likely to engage in activities that could compromise security for personal gain or other conflicting interests. This is particularly important in scenarios where financial or personal motivations could lead to security breaches. Allocation of roles and responsibilities promotes accountability within the organization. When individuals are held responsible for specific security tasks, they are more likely to take ownership of those tasks and ensure they are carried out effectively. This fosters a culture of accountability, which is crucial for maintaining security. The allocation of roles often goes hand in hand with resource allocation. It ensures that the right personnel, with the appropriate skills and training, are assigned to security-related tasks. This maximizes the efficient use of human resources in securing the organization. Segregated roles allow for the efficient and effective management of information security tasks. Different individuals or teams can focus on specialized areas of security, whether it's access control, incident response, or compliance monitoring. This specialization enhances expertise and leads to more robust security practices. Defining and segregating roles is a proactive measure to prevent inappropriate activities, such as unauthorized access, data breaches, or misuse of information.

- **Human Resource Security:** Effective Human resource security is a fundamental aspect of safeguarding an organization against insider threats. This includes employees, contractors, and temporary staff who have access to the organization's systems and data. By managing their lifecycle effectively, an organization can reduce the risk of insider-related security incidents, such as data breaches, theft, or sabotage. Effective human resource security begins with the onboarding process. Conducting background checks as part of the hiring process helps verify the credibility and trustworthiness of potential employees and contractors. This is particularly important when granting access to sensitive data and systems. Afterwards, employees and contractors are introduced to the organization's security policies, practices, and expectations. They receive training on cybersecurity awareness and their responsibilities in protecting sensitive information. Ongoing training and awareness programs are essential components of human resource security. These programs educate employees, contractors, and temporary staff about evolving cybersecurity threats, safe computing

practices, and reporting mechanisms for security incidents. Such awareness initiatives empower individuals to make informed security decisions. As organizational structures evolve, and new personnel are onboarded or roles change, human resource security practices must adapt accordingly. Flexibility and agility in managing the security lifecycle are essential to addressing emerging threats. Managing the exit of employees, contractors, or temporary staff is a critical aspect of human resource security. Clear termination procedures should be in place to ensure that all access privileges are promptly revoked, equipment and assets are returned, and data is securely handled. This helps prevent disgruntled individuals from causing harm after their departure.

- **Asset management**: Effective asset management begins with identifying and cataloging all the digital and physical assets within an organization. This includes hardware (e.g., servers, laptops, routers), software (e.g., applications, operating systems), data (e.g., databases, sensitive files), and even physical assets (e.g., access cards, security cameras). A comprehensive asset inventory provides clarity about what needs to be protected. For each asset, it is essential to identify an owner or custodian who is responsible for its security. This owner should be a person or department within the organization who understands the asset's value, vulnerabilities, and the security measures required to protect it. Assigning accountability ensures that asset owners are responsible for safeguarding their respective assets. They are held accountable for implementing security measures, monitoring for vulnerabilities, and responding to security incidents related to their assets. This sense of ownership promotes a proactive approach to security. Knowing who owns and is responsible for each asset is fundamental to implementing access controls effectively. Access can be restricted to authorized personnel based on their roles and responsibilities. Asset management provides the foundation for defining access policies. In addition to physical assets and hardware, asset management extends to data. Organizations should classify data assets based on their sensitivity and importance. This classification guides data protection measures, such as encryption and access controls.

- **Access control:** Access control is a critical component of information security. It ensures that only authorized individuals or systems can access sensitive information. By restricting access, organizations protect their data from unauthorized disclosure, tampering, or theft. Mechanisms, such as passwords, biometrics, and multi-factor authentication (MFA), help prevent unauthorized users from gaining access to systems and data. This is crucial in preventing data breaches and cyberattacks. Restricting network access and connections through network segmentation is a strategy to enhance

security. By dividing the network into segments, each with its own access controls, organizations can limit lateral movement by attackers if one segment is breached. Effective access control allows organizations to define fine-grained permissions. This means that not all users have the same level of access. Access can be controlled at various levels, from entire systems down to specific files or database records.

- **Cryptography**: Cryptography plays a pivotal role in preserving the confidentiality of data. Encryption is the process of converting plaintext data into ciphertext using cryptographic algorithms and keys, ensures that only authorized parties with the corresponding decryption keys can read the information. This is vital in protecting sensitive data from unauthorized access. Encryption is a primary means of safeguarding data both at rest (stored data) and in transit (data being transmitted over networks). It prevents eavesdropping and data breaches, making it extremely difficult for malicious actors to decipher encrypted data. Cryptographic protocols like SSL/TLS (Secure Sockets Layer/Transport Layer Security) are used to secure internet communication. They encrypt data exchanged between a user's web browser and a web server, safeguarding sensitive information during online transactions, login sessions, and data transfers. Effective key management involves generating, storing, distributing, and revoking cryptographic keys securely. Cryptographic keys are the foundation of encryption, and their protection is paramount. Cryptography serves as a robust defense against cyber threats such as data breaches, ransomware attacks, and man-in-the-middle attacks. It raises the bar for attackers, making it exceedingly challenging to compromise encrypted data.

- **Physical and environmental security:** Physical security focuses on safeguarding an organization's physical assets, including its premises, equipment, and data centers. It involves implementing access controls to restrict entry to authorized personnel only. This includes measures like locked doors, access cards, biometric authentication, and security guards. Physical perimeters and barriers, such as fences, walls, gates, and turnstiles, create a boundary around the organization's facilities. These barriers deter unauthorized individuals from gaining physical access to sensitive areas. Security cameras and monitoring systems are essential tools for physical security. They provide continuous surveillance of critical areas and serve as a deterrent to unauthorized access. Video footage can also be crucial for investigations in the event of security incidents. In addition to technological measures, physical security often involves the presence of security personnel. Security guards can provide a physical presence, perform access control duties, and respond to security incidents as they occur. Environmental Controls:

Physical security extends to protecting against environmental threats such as fire, floods, earthquakes, and power outages. Organizations implement measures like fire suppression systems, backup power generators, and environmental monitoring to mitigate these risks. Physical security and information security are closely intertwined. Physical access to servers, data centers, and networking equipment must be tightly controlled to prevent data breaches. The principles of access control, authentication, and monitoring apply to both physical and digital assets.

- **Operation security:** Operation security involves establishing detailed operational procedures and responsibilities for handling various aspects of an organization's information systems. These procedures help ensure that tasks are carried out consistently and securely. One of the key aspects of operational security is defending against malware threats such as viruses, ransomware, and Trojans. Organizations employ antivirus software, intrusion detection systems, and email filtering to detect and mitigate malware risks. Robust data backup and recovery procedures are essential to ensure business continuity and data integrity. Regularly scheduled backups, both onsite and offsite, help protect against data loss in case of system failures, disasters, or cyberattacks. Additionally, comprehensive logging and monitoring systems are deployed to track system activities and detect anomalous behavior or security incidents. Security Information and Event Management (SIEM) solutions are often used to collect and analyze logs for signs of security threats. Managing and controlling the installation and use of operational software is critical for maintaining system security. Unauthorized or unvetted software can introduce vulnerabilities. Organizations enforce software controls through policies and procedures. Moreover, timely patching of software and systems is crucial to address known vulnerabilities. Patch management processes ensure that security patches are applied promptly to prevent exploitation by cybercriminals. Organizations conduct vulnerability assessments and scans to identify weaknesses in their systems and software. Once vulnerabilities are identified, organizations develop and implement strategies to remediate or mitigate these risks promptly. Operation security often involves coordinating and facilitating audits and assessments of information systems. These audits help ensure that security controls are effectively implemented and aligned with regulatory requirements and industry standards.

- **Communication security**: Communication and network security management involves implementing a set of measures and controls to safeguard the confidentiality,

integrity, and availability of data during transmission. Encryption is a fundamental aspect of communication security. It ensures that data remains confidential while in transit. Secure protocols like SSL/TLS are used to establish encrypted communication channels over the internet, protecting sensitive information such as login credentials and financial transactions. Additionally, in order to prevent unauthorized access to network resources and data, communication security incorporates authentication and authorization processes. Users and devices are required to prove their identities before gaining access. Authorization determines what actions or data a user is allowed to access. Moreover, security technologies such as Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) are critical components of network security management. Firewalls establish a barrier between a trusted internal network and untrusted external networks, while IDS/IPS systems monitor network traffic for signs of malicious activity and can take actions to block or mitigate threats. Furthermore, VPNs create secure, encrypted tunnels over public networks like the internet. They are widely used for remote access and secure communication between geographically distributed offices, ensuring that data remains protected even when transmitted over untrusted networks. In addition to the measures mentioned above, Organizations often require secure methods for transferring files and documents. Secure file transfer protocols (e.g., SFTP, FTPS) encrypt data during transmission and provide authentication to ensure data is sent and received securely. Finally, communication security extends to email and messaging platforms. Secure email protocols (e.g., S/MIME) and end-to-end encryption in messaging apps (e.g., Signal, WhatsApp) protect the privacy of electronic communications.

- **System acquisition, development and maintenance:** This aspect of information security focuses on embedding security considerations into the entire lifecycle of information systems. It begins with defining security requirements during the initial planning and acquisition phase. Organizations identify the security features and controls necessary for protecting sensitive data and ensuring the system's resilience against threats. During the development phase of information systems, security is integrated into the software development lifecycle (SDLC). This includes secure coding practices, vulnerability assessments, and code review processes to identify and remediate security flaws before deployment. Secure coding guidelines, such as the OWASP Top Ten, are often followed to address common security issues. Organizations use secure development tools and environments to create and test software securely. These tools include static and dynamic analysis tools, penetration testing platforms, and secure coding libraries. Secure development environments are

isolated from production systems to prevent the compromise of sensitive data during development. Secure development frameworks, such as DevSecOps, emphasize the integration of security into the entire development pipeline. This ensures that security is not an afterthought but an integral part of the development process, allowing for continuous security testing and remediation. After deployment, it is crucial to maintain the security of information systems by promptly applying security patches and updates. Vulnerabilities discovered post-deployment must be addressed swiftly to mitigate the risk of exploitation. Finally, robust testing is an essential component of system development and maintenance. This includes not only functional testing but also security testing, which involves vulnerability scanning, penetration testing, and security assessments to ensure that the system is resilient to attacks.

- **Supplier relationships:** Organizations must assess potential suppliers not only for the quality and cost-effectiveness of their products or services but also for their commitment to information security. This assessment involves evaluating the supplier's security practices, certifications, and adherence to industry standards. Organizations should conduct vendor risk assessments to determine the level of risk associated with each supplier. This assessment should include evaluating the supplier's cybersecurity posture, data protection measures, and compliance with regulatory requirements. High-risk suppliers may require additional scrutiny and security controls. Suppliers often have access to sensitive data or systems of the organization. Information security in supplier relationships should ensures that suppliers handle this data with the same level of care and protection as the organization would. Data protection and privacy clauses in contracts dictate how data should be handled and safeguarded. Additionally, contracts and service level agreements (SLAs) with suppliers should be singed, including specific clauses related to information security. These clauses define the security requirements, responsibilities, and expectations of both parties.

- **Information security incident management:** This involves monitoring network traffic, system logs, and other sources to identify unusual or suspicious activities. Information security incident management begins with the detection and classification of security incidents are categorized based on their severity and potential impact. Once an incident is detected, it should be reported promptly to the organization's incident response team. Organizations establish a dedicated incident response team or designate individuals responsible for managing security incidents. This team is trained to assess and respond to incidents effectively, minimizing potential damage. The incident

response team assesses the reported incidents to determine their scope, impact, and urgency. This triage process helps prioritize incident response efforts. Immediate actions are taken to contain the incident and prevent it from spreading further. This may involve isolating affected systems, changing access credentials, or blocking malicious network traffic. After containment, the focus shifts to eradicating the root cause of the incident and recovering affected systems or data. Security patches may be applied, compromised accounts reset, and data restored from backups. Effective communication is vital during incident management. Internal and external stakeholders, including employees, customers, regulatory authorities, and law enforcement, may need to be informed depending on the incident's nature and impact. After an incident is resolved, organizations conduct post-incident reviews or "lessons learned" sessions to assess the effectiveness of their response. These reviews identify areas for improvement in incident response procedures, security controls, and training. Organizations should maintain well-defined incident response plans that outline procedures, roles and responsibilities, and communication protocols for various types of incidents. These plans help ensure a coordinated and efficient response during stressful situations. Finally, in order to be prepared for real-world incidents, organizations should conduct incident simulation exercises and drills. These exercises help incident response teams practice their skills and assess the effectiveness of response plans.

- **Information security aspects of business continuity management:** Business continuity management (BCM) involves developing strategies and plans to ensure an organization can continue its critical functions and operations during and after disruptive events, such as natural disasters, cyberattacks, or equipment failures. Information security is an integral part of BCM, ensuring the availability and integrity of critical data and systems. Information security continuity within BCM focuses on safeguarding information assets and ensuring the continued availability of essential data and systems during disruptions. This includes strategies to prevent data loss, maintain access controls, and protect against cyber threats that could compromise data integrity. Organizations should implement data backup and recovery mechanisms to create redundant copies of critical data. These backups should regularly be updated and stored securely, allowing for rapid data restoration in the event of data loss or corruption. Backup strategies should be considered both on-site and off-site storage for redundancy. Additionally, High Availability (HA) and Disaster Recovery (DR) Planning are key components of information security within BCM. HA solutions aim to maintain continuous system availability, while DR plans focus on recovering

systems and data after a disruption. These plans include defined recovery time objectives (RTOs) and recovery point objectives (RPOs) to guide recovery efforts. Moreover, the use of redundant systems and infrastructure usually adhere to minimize downtime. This involve deploying failover systems, redundant data centers, and backup internet connections to ensure that critical services remain available even if primary systems fail. Ensuring network redundancy is critical also. Redundant network paths and connectivity options help maintain communication and access to critical resources during network outages or disruptions. Finally, regular testing and drills of business continuity and information security plans are essential. These exercises help ensure that redundant systems, data backups, and recovery procedures work as intended. Testing identifies weaknesses and provides an opportunity for improvement.

- **Compliance**: Organizations are subject to various laws and regulations that mandate specific security practices and data protection standards. Compliance with legal and regulatory requirements is a fundamental aspect of information security management. For example, GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), and PCI DSS (Payment Card Industry Data Security Standard) impose stringent data protection and security obligations on organizations. Compliance efforts involve understanding these requirements, aligning security practices accordingly, and regularly monitoring and reporting compliance status. In addition to legal regulations, organizations often enter into contracts and agreements with customers, partners, and suppliers that specify security and data protection obligations. Ensuring compliance with contractual requirements is essential for maintaining trust and legal standing. Organizations must incorporate these requirements into their information security policies and practices. Regular security audits and reviews should be conducted to assess the effectiveness of security controls and ensure alignment with legal, regulatory, and contractual requirements. These audits could be conducted internally or by third-party auditors. Findings from these audits inform organizations about areas that require improvement and corrective actions. Some organizations appoint legal counsel or compliance officers dedicated to ensuring adherence to legal and regulatory requirements. These professionals provide legal guidance and monitor changes in laws and regulations that may impact information security practices. Achieving and maintaining compliance is essential for Organizations not only for legal and regulatory reasons but also for building trust with customers, partners, and stakeholders by demonstrating a commitment to protecting sensitive information.

4.1.3. How insurance premiums are calculated

The cost of cyber insurance can vary depending on the size and type of business, as well as the level of coverage chosen. Many insurance companies offer customized solutions to meet the needs of each business. While specific methods can vary among insurance providers, the following are common factors that influence the calculation of cyber insurance premiums:

1. **Industry and Business Type**: Different industries have varying levels of cyber risk. Organizations in industries with more sensitive data, such as healthcare or finance, may face higher premiums.
2. **Geographic Location**: The geographic location of the organization can also influence premiums. Areas with higher cybercrime rates may have higher premiums.
3. **Risk Assessment**: Insurers evaluate the risk exposure of the organization.
4. **Cybersecurity Measures**: Insurers inquire about the organization's cybersecurity practices.
5. **Third-Party Assessments**: Some insurers may require third-party assessments or audits of the organization's cybersecurity practices.
6. **Coverage Limits**: The level of coverage required by the insured plays a significant role in premium calculation. Higher coverage limits typically result in higher premiums.
7. **Deductible**: The deductible or excess amount, which is the portion of the loss that the insured must cover before the policy pays out, affects the premium. A higher deductible usually leads to lower premiums.
8. **Annual Revenue and Size**: The organization's financial size, including annual revenue and number of employees, can be a factor in premium calculation. Larger organizations often pay higher premiums.
9. **Coverage Add-Ons**: Organizations can choose additional coverage options, such as coverage for social engineering attacks or ransomware, which can increase premiums.
10. **Market Conditions**: Broader market conditions, such as the overall state of the cybersecurity insurance market, can influence premiums. When cyber threats are on the rise, premiums may increase.

11. **Past Claims History**: An organization's history of previous cyber incidents and insurance claims can impact premiums. Frequent or severe claims may lead to higher premiums.
12. **Accumulation Risk:** An organization may also use reinsurance and risk modeling to spread and mitigate the potential financial impact of large-scale cyber events. Additionally, insurers may develop strategies for diversifying their cyber insurance portfolio to minimize concentration risk.

4.2. The role of communication and collaboration between insured parties and insurance companies

Effective communication and collaboration between insured parties and insurance companies are fundamental pillars in the domain of cyber insurance. This sub-chapter explores the pivotal role played by open and transparent communication, as well as the importance of collaborative efforts between both parties. Such communication and collaboration are essential to ensure a seamless and mutually beneficial relationship, ultimately leading to enhanced risk management and tailored cyber insurance solutions.

Communication between insured parties and insurance companies commences right from the outset, during the application and underwriting process. Insured parties are required to provide thorough and accurate information about their cybersecurity practices, risk exposure, and past experiences with cyber incidents. Clear and open communication at this stage sets the foundation for an effective risk assessment process, enabling insurance companies to develop tailored coverage options that precisely address the unique needs and vulnerabilities of the insured party.

Throughout the policy term, continuous communication remains imperative. Insured parties must promptly inform insurance companies of any material changes in their cybersecurity posture or business operations that may impact their risk exposure. This ensures that the insurance coverage remains relevant and up-to-date, providing appropriate protection against evolving cyber threats.

Moreover, in the event of a cyber incident, effective communication between the insured party and the insurance company is crucial. Prompt reporting of the incident to the insurer facilitates the claims handling process and allows for a swift and efficient response to mitigate the impact of the cyber event. Collaborative efforts at this stage may involve sharing information on the nature and extent of the incident, facilitating forensic investigations, and coordinating response measures to restore normal operations.

The role of collaboration extends beyond the incident response phase. Insurance companies may offer risk management and cybersecurity support to insured parties, encouraging proactive measures to prevent future cyber incidents. This collaborative approach may involve sharing best practices, providing cybersecurity training, and conducting vulnerability assessments to identify and address potential weak points in the insured party's cybersecurity defenses.

In turn, insurance companies benefit from improved risk assessment and risk management practices through collaboration with insured parties. By gaining deeper insights into the insured party's operations and cybersecurity posture, insurers can refine their underwriting strategies and enhance their risk models, leading to more accurate risk pricing and tailored coverage offerings.

Overall, effective communication and collaboration between insured parties and insurance companies are vital components of a successful cyber insurance relationship. Transparent communication fosters an accurate risk assessment process, leading to customized and effective cyber insurance solutions. Collaborative efforts promote proactive risk management and improve cyber resilience, benefitting both insured parties and insurance companies. By fostering a cooperative and transparent approach, insured parties can proactively protect against cyber threats, while insurance companies can continue to offer relevant and comprehensive cyber insurance solutions in an ever-evolving digital landscape.

4.3. Process for Applying Cyber Insurance

Companies insure themselves with the term "cyber insurance" to protect themselves from the risks associated with cyber threats and security breaches in their digital space. The process of obtaining cyber insurance includes the following steps (Carlton, 2017):

- Assessment of needs: First, the company must assess the cyber threats and risks it faces. This can include identifying the data it needs to protect, sensitive customer information, and potential threats. Assessing needs is a critical step in the process of acquiring cyber insurance and must be done with care and detail.
- Identify data and resources: The company must identify what data and resources it deems critical to its operation. These may include sensitive customer information, valuable trade secrets, internal data, or anything else that may be of value to the company.
- Identify cyber threats: A company needs to identify the various cyber threats it may face, such as phishing attacks, data leaks, or other types of cyber-attacks.

- Vulnerability assessment: The company must examine the vulnerabilities in its system that may expose them to risks. This may include weaknesses in the cyber security firewall, inadequate access control procedures, or weaknesses in password management (Carlton, 2017). Vulnerability assessment is an important stage in the process of strengthening a company's cybersecurity. The basic stages to vulnerability assessment are analyzed above: (Baballe et al., 2023):
    - Identify vulnerabilities: First, you need to identify vulnerabilities in your cybersecurity environment. These can result from weak points in the network, non-updated software, inadequate security policy, or even human errors. Assessing vulnerabilities and taking steps to address them are critical to maintaining the security of a company's cyber and information assets.
    - Impact analysis: The company must assess the potential impact of cyber threats on its operation, including potential financial losses, reputation, and legal liability. These assessments will help the company better understand its cyber insurance needs and choose the right coverages to protect against cyber threats and risks.

4.3.1. Evaluation of the cyber insurance provider

The company should choose a cyber insurance provider that offers the best coverage for its needs. Cyber insurance policies may vary by provider. Choosing your cyber insurance provider is another critical step in the process of acquiring cyber insurance and requires careful evaluation. Let's expand the process:

- Research and evaluate providers: The company should research the various cyber insurance providers in the market. This includes gathering information about their history, the range of services they offer, their reputation, and their experience in cyber threat remediation.
- Coverages and Policy Programs: As cyber insurance policies vary, the company should carefully analyze the available coverages and policy programs from each provider. This includes coverage for outages, data loss, compensation for legal fees, and additional services such as data recovery and cybersecurity training (Baballe et al., 2023).
- Evaluating the terms and costs: In addition to the coverages, the company should consider the terms of the policy, such as the coverage fluctuation policy, and the

deductibles. Also, the company needs to consider the cost of cyber insurance and how to pay for it.

- Examine the experience of the provider: The company should investigate the experience of the provider in dealing with cyber threats. This includes checking their history of indemnification from cyber-attacks and their ability to provide the necessary support in case of crises (Aaltola, 2022).
- Discuss policy customization: The company may need to tailor its cyber insurance policy to its specific needs. Discuss with the provider the possibility of tailoring the policy to cover exactly what they need.
- Compare offers: Finally, before making a decision, it is important to compare and evaluate the offers from various providers, taking into account the coverage, terms, costs and experience of the provider interested in taking out a cyber insurance contract. The company will have to decide which coverages wants. This may include restoring damaged data, dealing with legal claims from customers, compensation for lost revenue, and other related coverage. Determining the coverages is an important step in the process of obtaining cyber insurance.

Choosing the right cyber insurance provider is critical to protect the company from cyber threats, as it will ensure that risks are effectively covered and support is in place in the event of a crisis (Aaltola, 2022).

4.3.2. Implementing a cyber insurance contract

Implementing a cyber insurance contract is a multifaceted process that demands careful planning and strategic execution. Let's expand the process:

- Application: The company will need to apply to the selected cyber insurance provider, providing detailed information about their business and their cyber insurance needs.
- Evaluation by the provider: The cyber insurance provider will evaluate the application and determine the cost of the policy based on the risks identified.
- Policy Purchase: If the company agrees to the terms and cost of the cyber insurance policy, then it can purchase it.
- Policy implementation: With cyber insurance in place, the company must adhere to the obligations contained in the policy, such as taking security measures and reporting any security breaches to the provider. Implementing a cyber security

policy is an important step in ensuring the company is effectively protected from cyber threats. Let's expand further:

a) Implementation of security measures: The cyber security policy should clearly define the security measures to be taken to protect information and networks. These may include installing advanced anti-virus, monitoring networks for anomalies, and implementing access policies.
b) Staff training: The company's staff must be informed and trained on the correct use of information systems and the recognition of cyber threats. The educational role is critical in addressing the human factor in cybersecurity.
c) Monitoring: The company must maintain monitoring mechanisms to detect and respond to potential cyber threats. This includes monitoring networks and activities to identify potential anomalies and take immediate action.
d) Breach Reporting: The policy should specify how to report any security breaches to the cyber insurance provider. This process must be fast and efficient to deal with potential attacks without delay.
e) Continuous policy review: The cybersecurity policy should be reviewed and updated regularly to respond to changes in the cybersecurity environment and discoveries from security breach incidents.

Implementing these measures helps maintain strong cybersecurity that protects the company from potential cyber threats (Fathi, 2019).

Chapter 5 - Guidelines for additional support of cyber insurance services

5.1. The Vital Role of ISMS in Cyber Insurance Support

In response to this growing threat landscape, many organizations have turned to cyber insurance as a means to mitigate financial losses resulting from cyber incidents. However, merely purchasing a cyber insurance policy is not enough to ensure comprehensive protection. The implementation of an Information Security Management System (ISMS) can play a pivotal role in enhancing the effectiveness of cyber insurance services. A well-established, implemented, consistently maintained, and continually improved information security management system in line with ISO/IEC 27001 can serve as a valuable source for gathering data and information relevant to a cyber insurance policy.

The policyholder could submit to the insurer as required all the results stemming from the ISMS, such as the metrics and data from its information security measurement initiatives and the outcomes of its risk assessment exercise (in alignment with ISO/IEC 27005) (ISO, 2018).

5.1.1. Planning

During the planning phase, the policyholder identifies and assesses risks and opportunities with the aim of ensuring the effectiveness of the information security management system in achieving its intended objectives, mitigating adverse consequences, and fostering continuous improvement. To achieve this, the insured establishes an information security risk assessment and treatment process, preserving pertinent documented data. This documentation encompasses the processes, identified risks and opportunities, as well as risk assessment and treatment plans, all of which can be disclosed to an insurer.

These risk treatment plans outline the measures deemed essential by the policyholder to diminish cyber risks, and such necessary controls find their documentation in the insured's statement of applicability (ISO, 2018).

5.1.2. Support

Individuals who are involved in establishing, implementing, maintaining, and continuously improving the ISMS, must be aware of the system’s key aspects such as the information security policy, an understanding of their roles in enhancing the system's effectiveness and the associated benefits of system’s performance, as well as an appreciation of the consequences of failing to adhere to the system's requirements. Information related to the training and awareness efforts of these individuals can be shared with an insurer.

Furthermore, the policyholder is responsible for determining the necessity of both internal and external communications relevant to the ISMS. Throughout the implementation, operation, and maintenance of the information security management system, the policyholder is tasked with generating the requisite documentation as outlined in ISO/IEC 27001 and any additional documentation deemed essential for the system's optimal functionality (ISO, 2018).

5.1.3. Operation

Throughout the operational phase, the policyholder is tasked with several key responsibilities. These include strategizing, executing, and overseeing processes essential for meeting information security requirements, along with the execution of initial plans and actions formulated during the planning phase.

Furthermore, the policyholder must maintain documented records to the extent necessary to ensure the proper execution of defined processes, manage changes, and take corrective measures to mitigate any adverse impacts as required. It is also crucial to manage outsourced processes, conduct periodic information security risk assessments, taking into consideration the criteria established during the planning phase, and retain documented records of these assessment results.

Additionally, the implementation of the information security risk treatment plan is vital, with the retention of documented records detailing the outcomes of this risk treatment. The documentation generated during this operational phase is available for sharing with the insurer (ISO, 2018).

5.1.4. Performance evaluation & Improvement

In the process of performance evaluation, valuable data regarding the effectiveness of information security controls, whether of a technical nature or otherwise, can be generated. This enables the insured party to compile and present information on the performance and efficacy of the implemented controls. Such data can be derived from various sources, including the

controls themselves, measurements taken of these controls, the application of metrics, or through regular monitoring, review, or assessment of both the controls and the processes they support.

Furthermore, internal audits of the information security function, controls, or the entire ISMS can yield additional insights into the efficiency and effectiveness of these components, while also providing contextual information for this data. Third-party audits, when necessary, can also be employed for data collection. To ensure ongoing suitability, adequacy, and effectiveness of the information security management system, management reviews are mandated at scheduled intervals.

The data acquired during the evaluation phase serves the dual purpose of identifying non-conformance and areas necessitating continuous improvement, and it can be documented as evidence of monitoring and measurement results, making it accessible for sharing with an insurer. Moreover, the evaluation of information security may reveal new risks or alterations in previously identified ones, which should be documented and communicated to the insurer.

In response to identified non-conformance, the actions undertaken can also contribute to the management of information security risks. It is imperative to document this risk treatment process and notify the insurer about the measures implemented and their impact. Additionally, the insured has the option to document the actions taken to enhance the suitability, sufficiency, and effectiveness of the information security management system.

5.2. Skills development by information technology professionals

5.2.1. Education and Awareness

Ongoing education and awareness are key elements for IT professionals as they face several important reasons that make it necessary. First, the IT space is constantly evolving, with new technologies and approaches appearing frequently. Education and awareness is the key for professionals in order to be prepared for latest developments and confront cyber-attacks. Training and awareness of cybersecurity best practices, threats and countermeasures are critical to protecting data and systems. Also, knowing the regulations and regulatory requirements regarding data privacy and security is an important aspect that requires attention from IT professionals, as many industries have strict requirements in this area. Compliance with these regulations is essential to avoid legal problems. IT professionals often face technical problems that require problem-solving skills (Kilic, 2012).

In addition, continuing education promotes innovation, enabling professionals to develop innovative solutions to business challenges. Continuous learning and awareness can also lead to career development, as many organizations value employees who invest in their professional development. Finally, technology is dynamic, and IT professionals must adapt to change with speed. Training and awareness help people embrace change, become familiar with new technologies, and adapt to changes in their work responsibilities.

Cyber security is not just an issue for IT departments. It is a collective responsibility that transcends organizational boundaries. As cyber threats continue to evolve and adapt, the need for a proactive, informed and vigilant approach becomes more apparent. Therefore, fostering a culture of cybersecurity awareness that spans all employees from the boardroom to the front lines is necessary (Bostan, 2015).

From ransomware and phishing to zero-day vulnerabilities and supply chain attacks, the arsenal of cyber threats is vast and ever-expanding. In order to face these challenges, it is necessary for IT professionals to be informed about the latest trends and developments in the field of cyber security is necessary.

Moreover, it is vital for organizations to invest in advanced cyber tools and solutions and to update and regularly review their incident management plans. This is explained from the fact that Cybersecurity is not a static endeavor, but a dynamic process that requires constant monitoring and adaptation to effectively prevent cyberattacks (Bostan, 2015).

5.2.2. Problem Solving Skills

Troubleshooting, is a crucial task for IT professionals as they often deal with complex technical issues that require problem solving skills in order to give immediate solutions to business systems. Their training and education provide the necessary knowledge and tools to recognize and effectively resolve these issues. In the ever-changing world of Information Technology (IT), problem-solving skills are essential to industry success. IT professionals, from technical support to systems architects, bear the critical burden of addressing and resolving complex technical issues that can disrupt operations, compromise security, and impede progress.

Education and training are the foundation upon which these professionals base their ability to deal with problems. These learning processes provide a deep understanding of technologies, software and hardware, making them necessary for problem solving. Top IT training programs and certifications provide hands-on experience and opportunities to simulate real-world problems, helping professionals improve their skills and familiarize themselves with the latest technologies.

IT troubleshooting is not just limited to technical expertise. It also requires effective communication and collaboration, as IT professionals often work in cross-functional teams. The ability to communicate technical issues to non-technical stakeholders is critical to problem solving and the proper functioning of teams.

Finally, IT troubleshooting requires constant updating and adapting to ever-changing technologies and challenges. Professionals must always be ready to learn and face new challenges, anticipating and preventing problems for the future (Kurmaiev et al., 2020).

5.2.3. Innovation

Education promotes innovation by exposing IT professionals to new ideas and approaches. Well-educated professionals are more likely to develop innovative solutions to business challenges.

The realm of Information Technology is intertwined with innovation, constantly striving to push the boundaries in our digital age. Education plays a key role in fostering and promoting innovation among IT professionals, acting as a source of new ideas, perspectives and approaches. Well-educated professionals are not only better prepared to deal with the complexities of their field, but are also more likely to understand and pioneer innovative solutions to the ever-evolving challenges facing business and society. Education is the foundation upon which innovation develops. Through formal education, IT professionals come into contact with a variety of concepts, theories and technologies. This exposure broadens their intellectual arsenal, enabling them to draw on a rich tapestry of knowledge when faced with problems. This allows them to connect different fields of knowledge, promoting creative thinking and new approaches to problem solving (Kurmaiev et al., 2020).

In addition, educational institutions often act as incubators for innovation. Research centers, laboratories and collaborative environments in universities and technical schools provide fertile ground for research and development of advanced ideas and experimentation with new technologies. Here, IT professionals have the opportunity to participate in research and development activities, leading the advancement of their industry. Furthermore, education is not simply about acquiring knowledge, but also about promoting critical thinking and openness to inquiry. IT professionals who have been trained in a rigorous educational environment are more inclined to overturn the established facts, challenge common paradigms, and seek innovative solutions. They have the ability to see obstacles as opportunities for improvement and growth (Bandyopadhyay, 2019).

Innovation in IT is not only limited to technology, but also extends to business processes, user experiences and social impact. Well-educated IT professionals are better

equipped to shape integrated solutions that address the technical domain while addressing broader business and societal challenges. This ability to think strategically and deal with the big picture is a hallmark of innovative IT professionals. Finally, innovation thrives in an environment where continuous learning and professional development are highly valued. IT professionals who understand the constantly evolving nature of their field and are committed to continuous learning have the ability to stay current on emerging trends and technologies. This approach encourages a culture of innovation in business.

5.2.4. Adaptation to Change

Technology is a dynamic field and IT professionals must be ready to adapt quickly to this constant change. Education and awareness help people accept this change, learn new technologies, and adapt to new roles and responsibilities.

In the fast-paced space of technology, constant change is the norm. IT professionals must be flexible, adapt quickly to innovations, compromising the accuracy of the resulting changes and upheavals. Education and awareness act as navigational gateways, guiding them through the constant waves of transformation and enabling them to not only face change but harness it for growth and innovation.

Technology, by its very nature, is a cycle of creation and transcendence. New programming languages, materials, software methodologies, and cybersecurity threats are constantly emerging, requiring IT professionals to remain prepared and receptive to these changes. Education acts as the means through which they acquire the knowledge and skills they need to navigate this dynamic environment. Education provides a solid foundation, allowing them to easily adapt to change and realize their potential for growth and innovation. Moreover, the training is not only limited to the technical aspect. It also includes a broader perspective. IT professionals gain insights into the business implications of technology change, enhancing their ability to align IT strategy with organizational goals. This comprehensive understanding fosters a culture of adaptability that extends beyond the technology itself.

Finally, adapting to change requires continuous learning and professional development. IT professionals who understand the ever-evolving nature of their field are more willing to pursue new learning experiences and acquire new skills. This approach encourages a culture of innovation in business. Education and awareness reinforce this approach, enabling IT professionals to stay current on emerging trends and technologies.

5.2.5. Networking

Attending educational events, conferences and workshops provides IT professionals with the opportunity to build professional relationships with colleagues and experts in the field. These meetings can lead to partnerships, mentoring, and career opportunities. Educational events, conferences and workshops represent more than just places where you gain knowledge. They are a framework where you can create important relationships, thus influencing your career path (Carlton et al., 2017).

Where the IT community comes together is at educational events, conferences and workshops, creating a vibrant ecosystem of interested people with a passion for technology. Through active participation and engagement, you can develop relationships with peers who share the same interests, challenges and aspirations. These relationships often transcend geographic boundaries, allowing you to tap into a global network of expertise. Additionally, networking provides a fertile ground for mentoring. You can connect with established experts and seasoned IT professionals who often participate as speakers, panelists or colleagues at educational events and conferences. Interacting with these experienced professionals can lead to mentoring relationships that provide valuable guidance, insights and advice for your career path. Mentoring is two-way and fosters a culture of continuous learning and growth (Carlton et al., 2017).

Finally, networking is not limited to face-to-face meetings. In the internet age, you can also form important professional relationships through online platforms and social networks. This complements one-on-one interactions and expands the reach of your professional relationships (Carlton et al., 2017).

5.2.6. Continuous Skill Development

In the ever-evolving field of information technology, staying up-to-date with the latest tools, programming languages, and technologies is essential. Ongoing education and skill development programs ensure that IT professionals can meet the demands of an industry that is constantly innovating. Whether through online courses, certifications, or workshops, these opportunities allow them to refine and expand their technical expertise. Educational initiatives often cover topics related to cybersecurity best practices, risk management, and threat mitigation. This knowledge equips IT experts to safeguard their organization's data and systems effectively. From Global Perspective, education programs may incorporate elements of cultural awareness and global business practices, preparing IT experts to excel in diverse and cross-cultural environments.

Lifelong Learning cultivate a culture of continuous learning within the IT community. IT professionals recognize that their industry is dynamic and that their knowledge should continually evolve. This mindset encourages them to seek out new learning opportunities independently and proactively.

In conclusion, education and awareness programs for IT professionals extend beyond technical knowledge, encompassing soft skills, ethical considerations, adaptability, problem-solving, cybersecurity awareness, global perspectives, and a commitment to lifelong learning. These multifaceted approaches empower IT experts to excel in their roles, navigate the ever-changing IT landscape, and contribute positively to their organizations and society as a whole (Kurmaiev et al., 2020).

Chapter 6 - Development of a framework of actions for leveraging cyber insurance services by public and private organizations

6.1. Presentation of the incident response management framework

The security incident impact management framework is a critical element in the development and implementation of cybersecurity services. It is essential to have a systematic framework that will allow us to effectively address security threats and incidents that may affect public and private organizations. In this context, we will examine the main aspects of the security incident impact management framework (Tropina et al., 2015).

This framework includes the following steps and components:

- Risk Identification and Assessment: First, we need to identify the potential cyber risks that organizations may face. This includes assessing IT system and network threats and vulnerabilities.
- Planning a Risk Management Strategy: Based on the identification of risks, we need to develop a strategy to manage them. This includes setting goals and selecting appropriate security measures.
- Implementation and Implementation of Security Measures: The next step is to implement the security measures that have been designed, including upgrading the technological infrastructure and training the staff.
- Monitoring and Evaluation: It is important that we continuously monitor the effectiveness of security measures and evaluate our response to security incidents.
- Review and Improvement: The impact management framework must be subject to continuous review and improvement. This includes evaluating proposals and adapting security measures to new threats and opportunities that may arise.

Proper implementation of this security incident impact management framework empowers organizations to effectively address cyber threats and ensure ongoing cybersecurity (Rosenzweig et al., 2019).

6.2. Strategies for effective collaboration and information sharing between public and private entities

Collaboration and information sharing between public and private entities are key strategies for improving cyber security utilization. Below are recommendations and suggestions for effective implementation of these strategies (Tropina et al., 2015):

- Create a Joint Coordination Body: Creating a joint coordination body between public and private organizations can be the center for collaboration and information sharing on cyber threats.
- Establishing a Common Information Sharing Platform: Developing a common information sharing platform can enable safe and effective exchange of information about threats and attacks.
- Creation of Joint Response Mechanisms: It is important to develop mechanisms that will allow an immediate and coordinated response to critical cyber threats.
- Strengthening Cyber Education: Training employees in cyber security is essential to counter threats. Collaboration between public and private companies can enhance education and awareness efforts.
- Facilitating the Exchange of Experiences: The public and private sectors must facilitate the exchange of experiences and best practices in dealing with cyber threats.
- Setting Common Priorities: Public and private agencies must work together to set common priorities in the field of cybersecurity.
- Strengthening the Legislative Framework: Cooperation may include strengthening legislation governing cybersecurity and data protection.

Effective collaboration and information sharing between public and private entities is critical to protecting critical infrastructure and addressing cyber threats. Only through this collaboration can we strengthen security in a world where cyber threats continue to grow.

It is important to emphasize that cyber threats do not recognize national borders, and for this reason cooperation between different states and sectors is essential. In addition, cyberthreats are constantly evolving with the rapid development of technology, and for this reason cooperation with the private sector is essential to counter them.

In this context, some of the key practices described in the text include:

- Integrating Partnership into National Policy and Legislation: It is important to have a clear demarcation of public and private sector collaborative relationships in national policy and legislation. This includes recognizing the

importance of these relationships in national cybersecurity policy and strategy.

- Participation of the Private Sector in Decisions: It is important to have the participation and input of the private sector in political, legislative and regulatory decisions that affect them. Their input can help develop effective policies and practices.
- Transparency and Oversight: The creation of transparency and oversight mechanisms for public-private partnerships is essential. These mechanisms ensure the smooth functioning of relationships and compliance with cybersecurity objectives (Rosenzweig et al., 2019).

6.3. Case studies – Real Examples of Collaboration between public and private sector concerning cyber insurance and cyber security

This section will present some good practices of cooperation between public bodies and private companies that highlight good practices in relation to public-private partnerships in the field of cybersecurity:

Czech Republic

The Czech Republic recognizes the importance of cooperation between many states and non-state actors in addressing cyber threats. It has adopted an integrated approach and ensures that private businesses, government authorities and citizens contribute positively to cyber security.

Denmark

Denmark is strengthening cooperation between the public and private sectors in the field of cyber security through practical actions that promote the exchange of knowledge and experience. These initiatives strengthen advisory efforts towards public authorities, businesses and citizens and contribute to the competitiveness of Danish companies.

Estonia

Estonia maintains an active and cohesive cybersecurity community. It opens technical channels of communication, organizes joint exercises and integrates the private sector and academia in the drafting of legislation and strategic planning. This contributes to their effective cooperation.

Finland

Finland recognizes that cybersecurity requires cooperation between many sectors of society, including government, the business community and citizens. It emphasizes the need for transparency in the public-private sector process and the management of supply chains for information security. In addition, it emphasizes the need to create a comprehensive structure that will take cyber security into account and ensure business continuity and incident preparedness. The management of supply network and supply chains plays an important role.

Italy

Italy adopts a "whole society" approach based on public-private partnership. This strategy includes collaboration with industry, culture, academia and the media. In addition, it emphasizes the importance of transparency, continuous consultation and awareness of cyber security.

Slovakia

Slovakia's National Cybersecurity Strategy (2021-2025): Slovakia emphasizes the importance of international cooperation and trust between public administration, private sector and academia for the development of cybersecurity.

Serbia

National Cyber Security Strategy of the Republic of Serbia (2021-2026): Serbia's strategy emphasizes that cooperation between the public and private sectors is one of the main pillars of cyber security. In addition, it highlights the importance of trust and increasing capabilities to protect information.

Turkey

Turkey's National Cyber Security Strategy (2020-2023). Turkey aims to develop collaborative efforts in the field of cyber security, encouraging the exchange of knowledge and experience between public and private sectors, as well as strengthening connections with stakeholders, especially young people studying in the field of cyber security.

These examples highlight the importance of public-private collaboration in cybersecurity and how it can be achieved effectively.

Greece

The National Cybersecurity Strategy of Greece for the period 2020-2025 includes policies, objectives and actions aimed at strengthening the country's cybersecurity. This

strategy is designed to protect networks, information systems and national interests from cyber threats and cyber-attacks. The details of this strategy may include the following:

- Critical Infrastructure Protection: The strategy focuses on protecting critical infrastructure, such as energy networks, telecommunications networks, and water systems.
- Strengthening Government Security: Efforts are focused on increasing the cybersecurity of government institutions and administrative networks.
- Strengthening cooperation with other countries and international organizations: Greece cooperates with other countries and international organizations to share information and assist in joint cybersecurity initiatives.
- Strengthening Awareness and Education: The strategy includes educational programs to increase government, business, and public awareness of cyber threats.
- Cybersecurity in the Private Sector: Businesses and the private sector are encouraged to strengthen the cybersecurity of their information systems and consider adopting insurance policies to cover cyber threats.
- Research and Development: Research and development projects are supported to develop new technologies and methods that can enhance cybersecurity.
- Cyber insurance policies: The government encourages the development of a market for cyber insurance products and attempts to formulate policies that promote insurance against cyber threats.

This is an overview of Greece's national cybersecurity strategy for the period 2020-2025. This is a dynamic field that is constantly evolving as cyber threats evolve, and the strategy faces new challenges.

Conclusions

In this day and age, businesses and organizations face a broad and evolving risk landscape in the form of cyber threats and risks. Cybersecurity is becoming one of the most important organizational challenges due to intense digital acceleration, increasing reliance on networked systems, and widespread use of advanced hacking techniques. It is vital that we manage cyber threats and risks because a successful cyber-attack can have a negative impact on an organization's operations, reputation and financial stability.

Due to the widespread and frequent occurrence of cyber-attacks, a proactive cyber security strategy is primarily required. Cybercriminals often exploit vulnerabilities in networks, software and user behavior to enter a system without permission.

Additionally, the interconnectedness of today's business environment on a global scale amplifies the potential impact of cyberthreats. Supply chains, information sharing platforms and collaboration platforms are becoming critical elements of modern business operations. Any breach in these interconnected ecosystems can impact many businesses, causing widespread disruption and losses.

In addition, businesses must now comply with legal obligations and industry standards. Globally, governments and regulatory bodies have recognized the seriousness of cyber threats and have imposed strict regulations to protect personal data, safeguard critical infrastructure and protect privacy. Violations of these rules can result in serious fines, legal consequences and risk to a business's reputation.

To achieve compliance and maintain stakeholder trust, businesses must proactively manage cyber threats. Integrating cybersecurity into risk management frameworks is an essential need in the modern business world. Cyber security is emerging as a potential solution to reduce financial losses and provide a level of protection against cyber threats.

During this study, we examined the multifaceted aspects of cybersecurity, considering its applicability, effectiveness, and limitations in today's business and organizational environment. This includes looking at key factors such as policy coverage, underwriting factors, claims management and the role of insurance companies in promoting cyber security awareness and best practices. In addition, the impact of cybersecurity on risk culture, risk transfer mechanisms and the overall resilience of organizations to cyber threats was assessed.

The development of public-private partnerships in the field of cybersecurity is a cornerstone for achieving national goals of security, economic development, and social progress. To this end, collaborative relationships are required to be clearly defined in national policies and/or legislation, including recognition of their importance in national cybersecurity policy and strategy. This also includes assuring how these partnerships contribute to national

security, economic development and social progress goals, the details of which can be included in relevant action plans.

In addition, it is important to ensure that relevant private actors are consulted on policy, legislative and regulatory decisions that affect them. This involvement of the private sector contributes to the development of effective policies and practices.

Finally, the need for transparency and supervision in public-private partnerships and related activities is highlighted. Creating mechanisms that ensure transparency and oversight helps ensure the smooth functioning of relationships and compliance with cybersecurity goals.

References

Aaltola, Kirsi & Ruoslahti, Harri & Heinonen, Jarmo. (2022). Desired cybersecurity skills and skills acquisition methods in the organizations. European Conference on Cyber Warfare and Security. 21. 1-9. 10.34190/eccws.21.1.293.

Abdelwahab, Ihab & Ramadan, Nagy & Hefny, Hesham. (2020). Cybersecurity Risks of Blockchain Technology. International Journal of Computer Applications. 177. 8-14. 10.5120/ijca2020919922.

Allianz Global Corporate & Specialty (2017), Allianz Risk Barometer: Top Business Risks 2017, Allianz Global Corporate & Specialty SE, Munich

Anderson, J., & Jain, A. (2018). Cyber Insurance and Risk Management. In Cyber Risk Management (pp. 73-97). Springer.

Avinash, Kumar. (2021). An analysis of information technology security job advertisements.

Aziz, Baharuddin & Suhardi, Suhardi & Kurnia,. (2020). A systematic literature review of cyber insurance challenges. 357-363. 10.1109/ICITSI50517.2020.9264966.

Baballe, Muhammad & Muhammad, Abubakar Sadiq & Muhammad, Abdulmuhaimin & Aliyu Yusif, Mustapha & Musa, Aliyu & Imam, Bello Abubakar. (2023). Management of Vulnerabilities in Cyber Security. 3. 14-18. 10.5281/zenodo.7779507.

Balawejder, Bartłomiej & DANKIEWICZ, Robert & Ostrowska-Dankiewicz, Anna. (2019). The role of insurance in cyber risk management in enterprises. Humanities and Social Sciences quarterly. 26. 10.7862/rz.2019.hss.33.

Bandyopadhyay, Tridib & Mookerjee, Vijay. (2019). A model to analyze the challenge of using cyber insurance. Information Systems Frontiers. 21. 10.1007/s10796-017-9737-3.

Blanke, Sandra & Nielsen, Paul & Wrozek, Brian. (2019). How Can a Cybersecurity Student Become a Cybersecurity Professional and Succeed in a Cybersecurity Career?. 10.4018/978-1-5225-5927-6.ch007.

Bodin, Lawrence & Gordon, Lawrence & Loeb, Martin & Wang, Aluna. (2018). Cybersecurity insurance and risk-sharing. Journal of Accounting and Public Policy. 37. 10.1016/j.jaccpubpol.2018.10.004.

Boran, Akerke & Bazarbayev, Sultanmakhmud & Mustafina, Azel & Musraliev, Nursultan & Abdukraimov, Bakhtiyar. (2022). DDoS attacks and cybersecurity.

Bostan, Atila. (2015). Impact of education on security practices in ICT. Tehnicki vjesnik - Technical Gazette. 22. 161-168. 10.17559/TV-20140403122930.

Carlton, Melissa & Levy, Yair. (2017). Cybersecurity skills: Foundational theory and the cornerstone of advanced persistent threats (APTs) mitigation. Online Journal of Applied Knowledge Management. 5. 16-28. 10.36965/OJAKM.2017.5(2)16-28.

Cinar, Cihan & Alkan, Mustafa & Dörterler, Murat & Doğru, İbrahim. (2018). A Study on Advanced Persistent Threat. 116-121. 10.1109/UBMK.2018.8566348.

Coalition (2021) Cyber Insurance Claims Report, Coalition, Available online at https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2021-07-Coalition-Cyber-Insurance-Claims-Report-2021-h1.pdf (Accessed at 24 November 2021)

Cyber Insurance Market Conditions Report (2021), Guidance as the cyber insurance market continues to harden (Author Farley, J.) Gallagher, Available online at: https://www.ajg.com/us/news-and-insights/2021/jan/2021-cyber-insurance-market-report/ (Accessed at 24 November 2021)

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79-98.

Dioubate, Balla Moussa & Daud, Wan & Norhayate, Wan. (2022). Cyber Security Risk Management Frameworks Implementation in Malaysian Higher Education Institutions. International Journal of Academic Research in Business and Social Sciences. 12. 10.6007/IJARBSS/v12-i4/12300.

Dogan, Berkay & Edwards, Kian. (2022). Impact of Ransomware Attacks on Enterprises within the Retail Industry. 10.13140/RG.2.2.29008.17928/1.

Drexler, Alejandro & Rosen, Richard. (2020). Correction to: Exposure to catastrophe risk and use of reinsurance: an empirical evaluation for the U.S.. The Geneva Papers on Risk and Insurance - Issues and Practice. 47. 1-1. 10.1057/s41288-020-00193-4.

Droppa, Martin & Harakal, Marcel. (2021). Analysis of Cybersecurity in the Real Environment. 1-7. 10.1109/KIT52904.2021.9583748.

Eling, Martin & Schnell, Werner. (2016). What do we know about cyber risk and cyber risk insurance?. The Journal of Risk Finance. 17. 474-491. 10.1108/JRF-09-2016-0122.

Everett, Cath. (2011). A risky business: ISO 31000 and 27005 unwrapped. Computer Fraud & Security. 2011. 5-7. 10.1016/S1361-3723(11)70015-X.

Farley, J. (2021) The 2021 Cyber Insurance Market continues to harden, Available online at: https://www.ajg.com/us/news-and-insights/2021/jan/2021-cyber-insurance-market-report/ (Accessed at 29 November 2021)

Fathi, Said & Hikal, Noha. (2019). A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises. JOIV : International Journal on Informatics Visualization. 3. 10.30630/joiv.3.3.241.

Ferland, Justine. (2019). Cyber insurance – What coverage in case of an alleged act of War? Questions raised by the Mondelez v. Zurich case. Computer Law & Security Review. 35. 10.1016/j.clsr.2019.06.003.

Franke, U. (2017),The cyber insurance market in Sweden, Computers & Security, Vol. 68, pages 130-144.

Franklin, Onyechere & Ismail, Mohamed. (2022). THE ZERO-DAY VULNERABILITY. 10.24924/ijise/2021.04/v9.iss2/65.76.

Furnell, Steven. (2021). The cybersecurity workforce and skills. Computers & Security. 100. 102080. 10.1016/j.cose.2020.102080.

Ghazouani, Mohamed & Medromi, Hicham & Sayouti, Adil & Benhadou, Siham. (2014). An Integrated use of ISO27005, Mehari and Multi-Agents System in order to Design a

Comprehensive Information Security Risk Management Tool. International Journal of Applied Information Systems (IJAIS). 7. 10.5120/ijais14-451138.

Gordon, L. A., & Loeb, M. P. (2012). The economics of information security investment. ACM Transactions on Information and System Security (TISSEC), 5(4), 438-457.

Granato, Andrew & Polacek, Andy. (2019). The growth and challenges of cyber insurance. Chicago Fed Letter. 10.21033/cfl-2019-426.

Hejase, Hussin & Kazan, Hasan & Moukadem, Imad. (2020). ADVANCED PERSISTENT THREATS (APT): AN AWARENESS REVIEW. 10.13140/RG.2.2.31300.65927.

Herath, Hemantha & Herath, Tejaswini. (2019). Copula Based Actuarial Model for Pricing Cyber-Insurance Policies. Insurance Markets and Companies. 2.

Howden Cyber Insurance Survey (2021), Cyber Insurance: A Hard Reset, Howden Broking, Available online: https://www.howdengroup.com/sites/g/files/mwfley566/files/inline-files/Howden%20Cyber%20Insurance%20-%20A%20Hard%20Reset%20report_1.pdfGeneva Association (2018). Cyber Insurance as a Risk Mitigation Strategy

Iguer, Hajar & Medromi, Hicham. (2014). The Impact of Cyber Security Issues on Businesses and Governments: A Framework for Implementing a Cyber Security Plan. 10.1109/FiCloud.2014.56.

Isaac D. Sánchez-García, Tomás San Feliu Gilabert, Jose A. Calvo-Manzano (2023),Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic mapping review, Computers & Security.

Junior, Abinel & Arima, Carlos. (2023). CYBER RISK MANAGEMENT AND ISO 27005 APPLIED IN ORGANIZATIONS: A SYSTEMATIC LITERATURE REVIEW. REVISTA FOCO. 16. e1188. 10.54751/revistafoco.v16n2-215.

Kesan, Jay & Hayes, Carol. (2017). Strengthening Cybersecurity with Cyber Insurance Markets and Better Risk Assessment. Minnesota Law Review. 102. 191-276. 10.2139/ssrn.2924854.

Kilic, N. & Metin, Bilgin. (2012). Importance of education in information technology governance. 65-68. 10.1109/LINDI.2012.6319463.

Kitsios, Fotis & Chatzidimitriou, Elpiniki & Kamariotou, Maria. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. Sustainability. 15. 5828. 10.3390/su15075828.

Kshetri, Nir. (2018). The Economics of Cyber-Insurance. IT Professional. 20. 9-14. 10.1109/MITP.2018.2874210.

Kurmaiev, Petro & Morozova, Liudmyla & Bondarenko, Olena & Husarevych, Nataliia. (2020). Cyber insurance: the current situation and prospects of development. Revista Amazonia Investiga. 9. 65-73. 10.34069/AI/2020.28.04.8.

Malyuk, Anatoly & Miloslavskaya, Natalia. (2016). Cybersecurity culture as an element of IT professional training. 205-210. 10.1109/DIPDMWC.2016.7529390.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A. and Yautsiukhin, A. (2017), Cyber-insurance survey, Computer Science Review, Vol. 24, 2017, pp. 35-61.

Meland, Per Håkon & Tøndel, Inger Anne & Solhaug, Bjornar. (2015). Mitigating Risk with Cyberinsurance. IEEE Security & Privacy. 13. 38-43. 10.1109/MSP.2015.137.

Mishra, Alok & Alzoubi, Yehia & Gill, Asif & Anwar, Memoona J.. (2022). Cybersecurity Enterprises Policies: A Comparative Study. Sensors. 22. 10.3390/s22020538.

Mulugeta, Henock. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. Risks. 11. 10.3390/risks11060101.

Naseer, Junath & Iyenger, N Ch Sriman Narayana. (2016). A Review on Distributed Denial of Service (DDoS) Mitigation Techniques in Cloud Computing Environment. International Journal of Security and Its Applications. 10. 277-294. 10.14257/ijsia.2016.10.8.24.

Noussia, Kyriaki. (2021). Liability Insurance in the Context of the COVID-19 Pandemic. icade. Revista de la Facultad de Derecho. 1-18. 10.14422/icade.i110.y2020.006.

OECD (2017), Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264282148-en

OSCE (2023). Transnational Threats Department (TNTD) Co-ordination Cell under the direction of Ms. Szilvia Tóth, Cyber Security Officer

Peters, Gareth & Shevchenko, Pavel & Cohen, Ruben & Maurice, Diane. (2017). Understanding Cyber Risk and Cyber Insurance. SSRN Electronic Journal. 10.2139/ssrn.3065635.

Ponemon (2019), Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age, Ponemon Institute, Available online at: https://www.ponemon.org/research/ponemon-library/security/managing-cyber-security-as-a-business-risk-cyber-insurance-in-the-digital-age.html (Accessed at 29 November 2021)

Rosenzweig, Paul. (2019). Cybersecurity, the Public/Private 'Partnership,' and Public Goods.

Sanchez Garcia, Isaac & San Feliu, Tomas & Calvo-Manzano, Jose. (2023). Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic mapping review. Computers & Security. 10.1016/j.cose.2023.103170.

Saxena, Neetesh & Hayes, Emma & Bertino, Elisa & Ojo, Patrick & Choo, Kim-Kwang Raymond & Burnap, Pete. (2020). Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. Electronics. 9. 1460. 10.3390/electronics9091460.

Singh, Anshuman & Gupta, Brij. (2022). Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms: Issues, Challenges, and Future Research Directions. International Journal on Semantic Web and Information Systems. 18. 1-43. 10.4018/IJSWIS.297143.

Smeenk, G. R. (2017). The role of information sharing in managing cyber security risks. Computers & Security, 68, 176-189.

Tøndel, Inger Anne & Meland, Per Håkon & Omerovic, Aida & Gjære, Erlend Andreas & Solhaug, Bjørnar. (2019). Using Cyber-Insurance as a Risk Management Strategy Knowledge Gaps and Recommendations for Further Research.

Tropina, Tatiana. (2015). Public–Private Collaboration: Cybercrime, Cybersecurity and National Security. 10.1007/978-3-319-16447-2_1.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102.

Whitman, M., & Mattord, H. (2019). Principles of Information Security. Cengage Learning.

Woldemichael, Hailye. (2020). Emerging Cyber Security Threats in Organization. International Journal of Information and Communication Sciences. 5. 19. 10.11648/j.ijics.20200502.12.

Woods, Daniel W & Moore, Tyler. (2019). Does Insurance Have a Future in Governing Cybersecurity?. IEEE Security & Privacy. PP. 10.1109/MSEC.2019.2935702.

Yamin, Muhammad & Katt, Basel. (2019). Cyber Security Skill Set Analysis for Common Curricula Development. ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security. 1-8. 10.1145/3339252.3340527.

Yuryna Connolly, Alena & Wall, David & Lang, Michael & Oddson, Bruce. (2020). An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. Journal of Cybersecurity. 6. 10.1093/cybsec/tyaa023.

NATIONAL CYBERSECURITY AUTHORITY. (2020, December). ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020 -2025. https://mindigital.gr/. Retrieved August 5, 2023, from https://mindigital.gr/wp-content/uploads/2020/12/%CE%95%CE%B8%CE%BD%CE%B9%CE%BA%CE%B7%CC%81-%CE%A3%CF%84%CF%81%CE%B1%CF%84%CE%B7%CE%B3%CE%B9%CE%BA%CE%B7%CC%81-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%B1%CC%81%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf

International Organization for Standardization. (2018). Draft BS ISO/IEC 27102 Information technology — Security techniques — Information security management guidelines for cyber insurance.