Deep Science Publishing
https://doi.org/10.70593/978-93-49910-74-4_7

DeepScience
Open Access Books

Chapter 7: Securing digital insurance platforms in the era of cyber threats

7.1. Introduction

Cybercrime is a rapidly growing threat globally. As society increasingly depends on the digital world and technology, there is a great diversity of cybercrime, from stealing credit cards to ransomware. One of the most attractive targets for cybercriminals is financial institutions, including insurance companies, due to the high value of the information they hold, the financial gains their loss may bring, and the interconnected regulatory frameworks that make their impact hard to control. The pandemic has further favored cybercriminals having changed normal work patterns and brought many activities online without proper cyberprotection. For most companies and societies, cybersecurity is nowadays the main concern related to their digital transformation process (Almorsy et al., 2016; Fernandes et al., 2016; Conti et al., 2018).

Insurance is the only financial service that manages the risk of loss, damage, or injury to others. Its mechanisms guarantee transparency, sustain mutual trust, and guarantee the availability of needed resources. Cybersecurity insurance is a type of policy purchased by enterprises vulnerable to online attacks, that transfer the financial risks and losses of specific events to the insurer by paying a premium. Nowadays, however, the need for insurance against cybersecurity risks is being questioned. As the number and complexity of attacks have been on the rise and incidents have presented a lack of coverage many times, traditional market solutions may not be enough.

Insurtech companies are entering the traditional insurance market and promoting a new generation of insurance technologies and shifting insurance processes to the digital universe. Still in its early development stage, insurtech operates on the digital transformation also of the insurance market and its value proposition is predicated on having a technology to tackle the inefficiency of selling and servicing insurance products. The main motivation is to present an exploratory analysis of the cybersecurity

challenges of digital insurance platforms based on original interviews with European insurance companies and startups (Popovič & Hocenski, 2010; Kshetri, 2017).

7.1.1. Purpose and Scope of the Study

The upsurge of digitalization has proudly asserted itself in many sectors such as commerce, banking, and communication due to the impressive benefits of digital solutions over traditional ways of conducting business. Among those, the insurance market has increasingly embraced Digital Insurance Solutions to support and enhance customer experience, including Customer Engagement Platform, Data Analytics Platform, Business Process Management and Resource Management Platform, Online Insurance Platform, and Insurance Application Programming Interface. However, the nature of services provided by these solutions together with the financial resources at stake makes such platforms prey to cybercriminals, which have come up with an arsenal of sophistication and lethal weapons to exploit even the most secure environments.

Fig 7 . 1 : Securing Digital Insurance

Throughout the journey of implementing secure digital insurance solutions, it has been impossible to prevent some security attacks - such as data breaches and identity theft – occurred, causing irreplaceable damage to all parties involved in the insurance ecosystem, along with their partners and related parties. The malpractice utilized by attackers indicates that the current cybersecurity paradigm applied to insurance information systems cannot grant the necessary protection. So, the objective of this study is to suggest a new perspective regarding the cybersecurity of digital insurance solutions, calling for a shared responsibility paradigm among all involved parties regarding the security of digital insurance solutions and paving the foundations for measures that can be taken by cyber insurance buy-side and provider side to decrease the likelihood and impact of digital insurance solution cyberattacks. With the surge of digital insurance solutions, the cybersecurity of such platforms has called for growing attention due to the implications of cyber threats. Different from traditional cybersecurity external frameworks, such as protection, deterrence, detection, and reaction, the special nature of cyber insurance solutions leads to a complex capability landscape that encompasses all relevant actors – including insurance companies, customers, suppliers, insurance regulators, brokers, and cybersecurity framework - contributing to and influencing the propensities of company parties and the ecosystem as a whole toward external cybersecurity posture.

7.2. Understanding Cyber Threats

Threats posed by entities external to the digital system have grown radically since the birth of cyberspace. The consensus is that these have grown both in diversity and scale. In mid-2021, ransomware attacks accounted for 10% of all reported cyber breaches. Many insurance providers are reporting hundreds of millions in losses. The total economic cost of cybercrime is estimated to be at least $1 trillion a year, with only a tiny fraction of it being insured. While all infrastructure has an exposure, public pole infrastructure, logistics services, energy grids, chemical plants, and other critical infrastructures are a primary target. For critical public infrastructures, a successful ransomware attack could cost society much more than the ransom, with attendant effects on public health.

Cyber attacks manifest themselves in a variety of damaging ways to the insured. Cyber incidents can disrupt the normal course of business of entities. They can involve unauthorized access and data leakages of residential and commercial policy or motor databases. They can manipulate transaction or process controls. They can release malware or other harmful code. They can disrupt access or corrupt data. Cyber incidents can even deploy ransomware to hold systems hostage and require clients to pay ransomware to regain access to them. Attacks and incidents can be caused by multiple

and often unpredictable forces, making it difficult to prepare for, prevent, or respond to them and their effects. These include hacktivism, disinformation, nested cyber attacks, insider threats, supply chain risk, cyber terrorism, cyber deception, sabotage, state threats, social engineering, state-sponsored espionage, and advanced persistent threats.

7.2.1. Types of Cyber Threats

The different types of cybersecurity threats to organizations and individuals could be Phishing, Malware, Spyware, Ransomware, Data Exfiltration, Bots, DNS Spoofing, DDoS, Man-in-the-middle, etc. Phishing is a method of impersonation, using email or other mode of communication, to trick users into clicking on malicious links or providing confidential information such as login credentials and account numbers. Although phishing is primarily associated with email, other modes of communication, including text and direct messages on social media, also have been used successfully. Phishing attacks are sometimes the first step in more sophisticated attacks; attackers could use information gathered through phishing to organize cyber-attacks. Organizations need to train employees on how to recognize phishing attempts and respond appropriately. However, the sophistication of phishing attacks is increasing, making it more difficult to recognize them. Malware is a catchall term used to describe any harmful software, including viruses, spyware, adware, Trojans, and worms. Spyware is software that is installed to monitor user activity and gather sensitive information. Spyware can also be used to monitor activities that occur on the infected device, including keystrokes and information submitted via forms. Ransomware is malicious software that encrypts systems or personal files, making them inaccessible until a ransom has been paid. Data Exfiltration occurs when a malicious actor removes, or exfiltrates, data from a computer or network. Bots are malicious applications that run automated tasks that carry out commands or processes on behalf of the attacker. However, malicious bots often perform repetitive tasks to compromise systems or data, leading to denial of services. DNS Spoofing attacks provide an easy and effective way to target organizations and may be used to redirect targeted users to fake sites where their data can be stolen. It can also be accomplished by altering a web cache, compiling a list of IP addresses and hostnames, and guesswork.

7.2.2. Impact of Cyber Threats on Insurance

Insurance is based on quantitative risk assessment and premium development using historical data. If historical data does not exist or is not characteristic of the new type of risk, and if the risk is developing quickly, risk assessment becomes very difficult; it is uncertain if any premium can be charged which would make the product financially

viable or if the worst case scenario is much worse than current estimates. Such new, emerging risk situations exist especially about cyber risks. The development of new types of liability cover or product lines such as cyber risk coverage can in some cases be seen as "pioneering". New markets and new types of risk require from the insurance industry a balance of speed, accuracy, and prudence. Until the global insurance community has gained and mustered enough relevant, sufficiently detailed data, it will be hard to evaluate new cyber risks. Furthermore, it is important to ensure that the right questions are addressed when designing security measures for risk mitigation solutions. As the need for cyber security solutions in the economy increases, this in turn leads to increasing potential revenues for the insurance industry by providing the necessary coverage for cyber-related risks that customers require.

Insurance coverage is also often taken as a possible protection measure, making security considerations less demanding. If the risk is "outsourced" to the insurance company, the "owner" may decide that certain hack or data loss strategies are not worth countering and forgo taking any protective measures at all. This can be especially true within the financial industry and it has been shown that insufficient security measures increase the probability of an attack. This has been referred to as the "moral hazard" problem.

7.3. Digital Insurance Platforms Overview

The insurance industry is experiencing transformation driven by the need to respond to new market and customer needs. Companies and customers alike are increasingly adopting a digital-first approach. For insurance carriers and brokers, this transition means offering fully digitalized services—such as portals, applications, and policy administration—and using advanced technologies—cloud computing, big data, data analytics, artificial intelligence, natural language processing, and machine learning—for these services to drive operational efficiency. A part of the industry transition is the launch of digital insurance platforms. Generally, a digital insurance platform is a single entry point into an ecosystem of services and partners and combines multiple insurance plus non-insurance services.

Digital insurance platforms provide direct access to multiple capabilities including core insurance functions, such as policy administration and underwriting or partner ecosystem connections, or cross-industry functions, such as regulatory compliance and risk and fraud analytics. Such a platform aims to drive increased efficiency for carriers and deliver a superior customer experience through a faster, simpler process for policy issuance. It also aims to enhance customer retention and reduce the frictional costs associated with ownership through automated support for policies and claims.

Building such a platform required the redefining of key capabilities used to support digital technology, operating environment, organizational structure, governance model, and other technology areas. It also raised considerations about the core insurance functions central to the design of a digital insurance platform, of locating, integrating, and operating those functions versus leveraging existing policy administration capabilities. The decision to utilize existing core capabilities would likely limit the ability of insurers to create that truly seamless customer experience. Indeed, several carriers have announced they will be abandoning traditional policy administration systems altogether.

7.3.1. Architecture of Digital Insurance Platforms

Digital Insurance Platforms (DIP) have emerged as a frontrunner in the monetization race of the insurance industry in the new normal propelled by the pandemic. Leaders are embedding digital insurance functionality into their traditional business applications while looking to newly reformed external insure-tech companies to guide them in developing more comprehensive platforms from scratch. In essence, the DIP serves as a technology-driven core enabling technology companies to leverage finance by spurring the introduction of multi-niche complementary digital products and catered-for services from insurers and ancillary partners, further deepening relationships with customers through closed-loop offerings that utilize predictive analytics. By creating a unified ecosystem of API-enabled niche insurers that act like digital grocery stores for short-term or considered “low value” or digital retail dispositions, DIPs are creating a decentralized digital insurance hub around which activities and services to seek information, compare ratings, purchase, pay for, renew, claim for damages, review/evaluate experiences, spread the word about, and get advice for personal lines revolve.

DIP constellations provide customers with a one-stop shop making a multi-purchase of similar insurance coverage simpler, helping find discounted premiums, and added services, enabling online instant comparisons, and giveaways, and the additional reassurance that the insurance company has a track record for quick claims processing, and takes customer usability and experience as a priority. Digital platforms will allow the creation, investment, and interaction of the DIP inclination that can increase the network effect, lowering information asymmetry by integrating smart contracts on the blockchain for quicker and costless policy underwriting procedures. Acting individually or in a consortium can also help blockchain DIPs manage risk-sharing pools more effectively, using Internet of Things devices to capture and enhance data evaluation inputs, and bringing on board customers more adept at crowdsourcing.

7.3.2. Key Features and Functions

As a marketplace for the purchase, use, and delivery of insurance products and services, cyber insurance digital platforms help provide requests for insurance coverage and resolve claims. These key information exchanges involve multiple parties: the policies' issuers, customers seeking protection, third-party risk providers, and an overseeing party. The entire cyber insurance experience journey can be defined in 11 stages for 5 main participants.

We can group these activities into two big functions performed by the digital platform: a marketplace function and an orchestration function. The marketplace function is formed by six activities enabling interactions between clients, insurers, and vendors, similar to those from most digital marketplaces. The digital platform, by facilitating those interactions, provides added value to the clients and the insurers. The marketplace function alone cannot deliver the desired level of cybersecurity protection, since it does not deliver any jurisdiction or any guarantees. To deliver such a level, the platform needs to orchestrate the insurance journey, the chronological sequence of steps each participant needs to execute to receive or provide an insurance service and benefit. Orchestration is composed of the remaining five activities of the insurance journey. It functions like an intelligent process supposing, guiding, and controlling the interactions within the marketplace and its participants.

7.4. Regulatory Landscape

InsurTech accelerated the digitization and creation of online insurance platforms. Rapid digitalization prompted the urgency of data protection and cybersecurity. Cybersecurity, being a tech-related term, started emerging in regulatory discussions, primarily in economic sectors where the core business was heavily relying on or emerged from the digital world. As it is found in other areas or sectors of the economy, regulations need to be put in place to ensure trust in InsurTech innovation and digital transformation. Especially regarding data privacy and protection of sensitive personal and corporate customer data, its protection is of utmost importance in the highly regulated and sensitive insurance market. National and supranational regulators in countries like Germany and the UK as well as in the EU have put in place a regulatory framework. Cybersecurity has started turning into a public interest enforcement issue, as the available regulatory framework has increased.

In this section, we briefly discuss the important ones like the GDPR and the NIS Directive. We further focus on the impact of cyber risk regulations on InsurTech and online digital platforms to prove our thesis that InsurTech is at the same time an enabler and an obstacle for better cybersecurity in the insurance sector. Regulations like the

GDPR provide stringent rules for data protection but have also been subjects of discussions regarding their impact on cybersecurity. On one hand side, the requirements aim to increase data security measures but on the other hand, they create constraints for innovation and transformation of companies and thus lower the overall level of cyber risk protection. Other regulations like the NIS Directive or also the DORA but mainly NIS have direct cybersecurity implications and create strict reporting and compliance requirements.

7.4.1. Compliance Requirements

In recent years several regulatory bodies issued different regulations, acts, or other legal frameworks that outline industry guidelines and principles regarding data protection and cybersecurity. The recommendations include the application of the European General Data Protection Regulation and its main requirements. Emphasis is placed on the importance of various standards and offers compliance with different requirements. Recommendations also include the implementation of a Cybersecurity Framework.

The presented options are a non-exhaustive collection of the most important regulations that guide digital insurance compliance. For example, certain regulations are mandatory for organizations that process certain types of payment cards, while others outline data protection requirements for insurance companies that process data of customers with healthcare policies. Additional regulations require financial institutions to develop a written information security plan and to conduct annual risk assessments. Additionally, privacy by design is mandated, as well as the right to portability, the right to explanation, and the right to be forgotten, among others. Adherence to the mentioned regulations will help achieve legal compliance, but digital insurance companies still need to implement further regulatory requirements to ensure that they are prepared for potential cyber threats.

7.4.2. Impact of Regulations on Cybersecurity

Organizations across industries have been tasked with securing their information systems by various regulations. This includes annual risk assessments, strict controls, and the reporting of incidents. Governments, regulators, rating agencies, and boards of directors that previously focused on financial, operational, and safety performance now require information on cyber risk and management. On the other hand, as more organizations invest in cybersecurity programs, the cyber threat landscape will change, requiring increased vigilance and investment by everyone to defend against more sophisticated attacks. There is concern that regulatory compliance is not enough and regulatory guidelines may not keep pace with rapidly changing technology.

Even regulations that do not specify cybersecurity requirements may have cybersecurity implications. Privacy breach notification rules and regulations, compliance requirements, cybersecurity guidance, and state insurance cybersecurity regulations have all introduced various new requirements. Because these various rules and regulations do not cover the entire cybersecurity landscape individually, organizations must understand how to manage cybersecurity risks that are also not regulated by these rules or regulations. National standards bodies have created comprehensive cybersecurity management frameworks to assist organizations in understanding their cybersecurity risks. Their guidelines serve as a roadmap for organizations aiming to comply with existing rules and regulations and can assist organizations that are not required to comply with any existing rules or regulations in operating in a more security-centric manner. Moreover, their guidelines can help regulators understand an organization's cybersecurity posture and lend assistance in the event of a cyber incident.

7.5. Risk Assessment Framework

While there is broad alignment on the selection of techniques to assess risk, choosing when to assess risk, as well as how frequently sets organizations apart. While some organizations will assess risk periodically, too big a gap could result in actions taken aboard a ship that are out of sync with changes to risk on the ship and at the helm of the ship; other organizations take an approach that increases frequency in a triggering event-driven manner as things happen aboard the ship, at the ship's helm, on the waters the ship traverses, and on the weather. Driven more by simple cost-benefit considerations, consensus recommends adherence to periodic schedules. At the other end of the spectrum though, assessment processes can be modified in response to changes in the organization's activities and circumstances. For more mature organizations, assessments can be triggered by the introduction of new business processes, acquisition of new assets, development of new information resources, introduction of new technology, and changes in organizational structure or personnel. For organizations relying heavily on external vendors to deliver critical information services; or organizations that are highly dynamic, assessments can be frequently triggered by reports that information resources, technology, or security policies have been compromised. A fundamental dilemma as organizations launch into different waves of transitions to the cloud on the road to digital transformation is the tradeoff between reducing transition and threat and vulnerability identification and assessment costs associated with having fewer systems and data to protect versus escalating the costs of a cyber event tied to their increased reliance on a few cloud vendors compared to having many different provider partners.

Consistent with the priorities articulated in the framework, organizations achieve the biggest wins in limiting risk exposure by identifying their important systems, user data,

and assets that are most attractive to cyber intruders. Determining the importance of a system or asset for an organization's operations may be critical for understanding an organization's business impact in case of a cyber event. This type of assessment is traditionally made by the business, in consultation with IT, but as events have shown, sometimes the business is not fully aware of what would be required. Working closely with business leads to a more realistic understanding during incident response and recovery but these relationships are hard work.

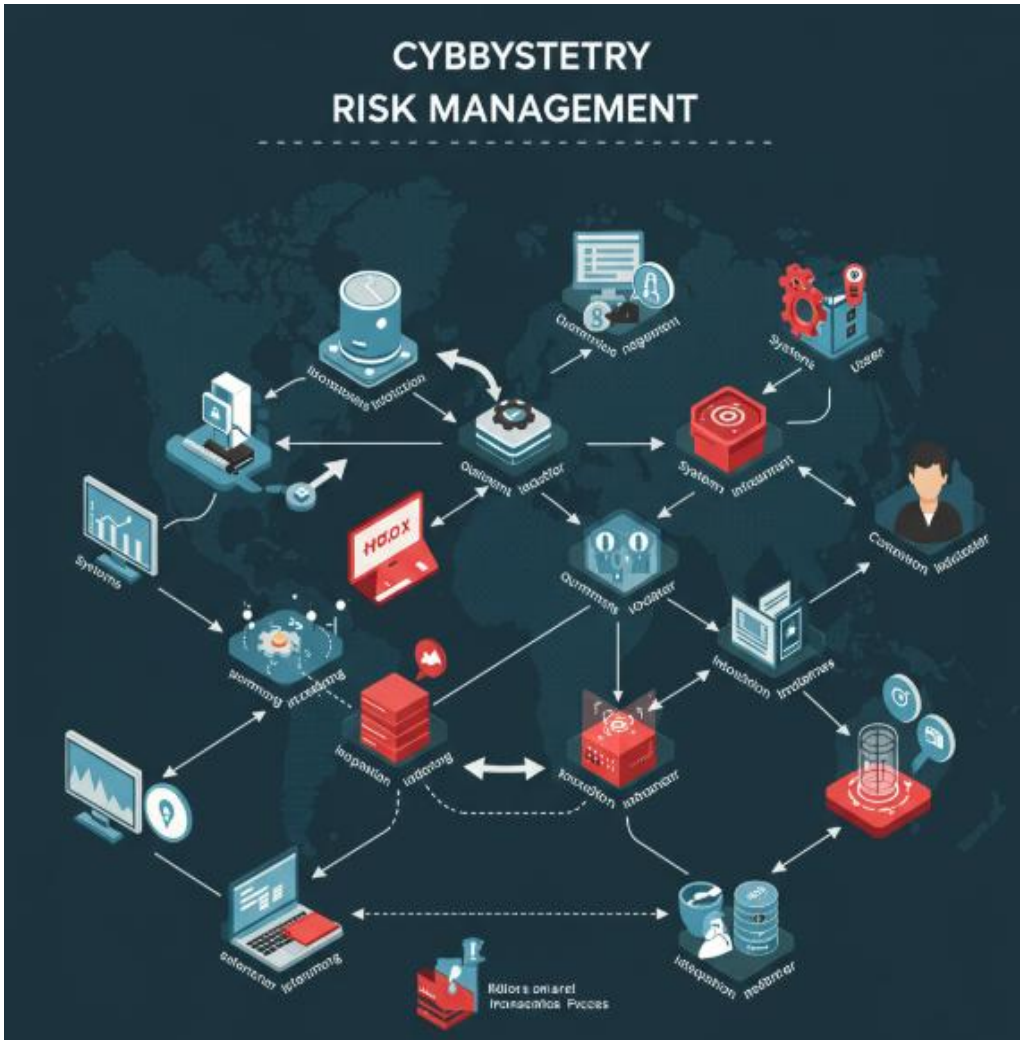

Fig 7 . 2 : Cybersecurity Risk Management

7.5.1. Identifying Vulnerabilities

Identifying vulnerabilities is a critical and daunting process for organizations and their related digital insurance platforms, as it involves reviewing hundreds of security controls, many of which are shared across multiple laws, regulations, and industry standards as well as technical standards and guidelines. Technology systems are only as secure as their weakest components or layers. Therefore, organizations must account for all potential concerns and spend additional time and money to address those concerns. Furthermore, an organization may have some unique business reasonably outlined in the corporation's risk assessment. There is no single source that can be relied upon to identify all reasonable business concerns without the need for additional review.

A comprehensive and effective vulnerability management and remediation program leverages regulatory and legal requirements, industry standards and best practices, actual vulnerabilities identified across the technology environment, and threat intelligence to prioritize and remediate the most critical vulnerabilities promptly. People will quickly forget that anyone was fired, that anyone was injured, or that anyone was badly distrusted. If regulations and contracts with third parties have communication planning requirements, the organization must comply with those requirements when reviewing established policies and where additional protocols for the technology program may be necessary.

There are numerous security standards and guidelines; however, few organizations have the resources to achieve compliance with all of them. Each organization should complete a formal risk assessment that aligns with its organizational culture and risk tolerance for its security program and related employees. Such assessments must be regularly updated at least annually and more frequently when there are any major changes to the technology environment or business model. Still, any unique concerns for the technology risk impact on the digital insurance platform and data should be documented for further review.

7.5.2. Assessing Threat Levels

Data breaches are practically a given for organizations these days, and preparing for one is a fact of life. Taking preventive measures early on before a breach enables you to recover sooner afterward, and indeed, even stop the breach in the first place. Understanding threat levels must include an examination of a broad array of dangers, for one organization may be subject to very high levels of one kind of threat while being immune from others. Auto manufacturers could be very concerned with product tampering or illicit interference with onboard electronics or facility security posing greater dangers than a data breach. Large retail companies might be most concerned

about credit card fraud, while even given their immense market power, witnessing a data breach to data on customer retail habits isn't unheard of. Those financial institutions most known for their privacy competencies should be especially cognizant of how identifiable breaches could create other indirect problems for their customers or reporting agencies.

Threat levels pose levels of risk in terms of monetary issues but have additional implications for corporate reputations. The question of possible breach and its impact is a major consideration involved in the writing up of predictions or other future statements required by regulations. Fines levied against firms for detected breaches have been increasing rapidly since regulations began in earnest. Companies have had data breaches resulting in identity theft in varying amounts, raising shareholders' eyebrows in concern. In some instances, the data breach was uncovered to have occurred for several years before disclosure, creating worst-case scenarios, which eventually may lead potentially to class action lawsuits.

7.6. Cybersecurity Strategies

Cybersecurity initiatives will only be effective if they are adequately planned, implemented, and enforced. Cybersecurity should be an integral part of a digital platform policy, incorporating definitions, guidelines, and security controls. In the same way that we wouldn't build a home without a solid foundation, neither should we design a digital platform that lacks a security plan. Organizations should consider working with experts in the area, as well as taking into consideration compliance requirements. A good cybersecurity policy will determine how and when to implement controls, continuously monitor the network, properly react if a cybersecurity event occurs, and analyze deficiencies in the policies afterward and correct them.

Digital insurance platforms should implement a preventive approach, as much as possible, to avoid, or at least minimize, disruptions to their operations. Organizations should take into account the use of business continuity plans, cybersecurity frameworks, and network segmentation. In the event of a cybersecurity event, organizations should define a set of procedures to follow (technical and operational), including detailed incident classification criteria (time, victim, type of threat, type of attack, severity, degree of impact, stop/operate), the assignment of responsibilities to properly handle an incident (including a communication plan to employees and/or clients), established communications systems to be used during the incident, and determination of when and how to stop services not affected by the incident and how to recover those services in an orderly and secure manner.

7.6.1. Preventive Measures

Digital insurance platforms are a popular target for cybercriminals because they house sensitive data that is sold for high prices. Insurers must secure their websites to protect themselves from hackers and a possible loss of reputation and business and ensure they can respond in case they experience an attack. Cyber risk is not only a threat to insurers; insurance against cyber risk has become a necessity for many companies in various sectors. Technical, physical, administrative, and legal preventive measures can help prevent attacks against digital insurance platforms. Responsibility for loading information on digital insurance platforms is usually shared between the client and the insurance firm: Both should check the information that is published by the other on the website to verify it is correct. The insurance firm should also share expertise on potential security threats with clients. Insurers must have a competent IT team responsible for minimizing cybersecurity risks. Dedicated cybersecurity measures should be implemented, including encrypting sensitive client information, regularly changing digital certificates, authentication security systems, firewalls, antivirus applications, and intrusion detection systems. Proper website and database security for sensitive client information should be ensured. Insurers must also inform clients through security protocols and warning messages about digital attacks, and make sure that are updated. Audits of the digital insurance system must be done both regularly and whenever a new service is implemented to remedy weak points. Another recommended measure is the establishment of a External Security Testing program that uses trusted ethical hackers to find solutions against security threats. Finally, a Business Continuity Plan must be prepared to reduce potential damage from attacks.

7.6.2. Incident Response Plans

The capacity to respond to security incidents in an organized fashion is an invaluable asset. Organizations should have incident response plans that include escalation procedures for incidents of different levels; guidelines for addressing service or product disruptions; and guidelines for notification to the trusted third-party incident response team. Testing incident response plans with simulated incidents is essential for contractors and organizations to demonstrate readiness in case of a real breach incident. An organization’s response strategy should include forgiveness policies and rules of engagement to encourage and enable incident reporters to cooperate fully with the identification of intrusions and response procedures. Cybersecurity incident scenarios could involve hackers threatening to announce breaches at a certain date unless paid a ransom; hackers threatening to put inserted malware on a website unless a ransom is paid; hackers using malware timed to trigger on a certain date if not paid a ransom; and service disruption at indie websites on a certain day unless paid a ransom. Intrusions into

the security of contractual mandates could be detected through regular vulnerability scanning of encrypted transaction processing routines, vulnerability scanning of incorporated third-party services, security audits of website software, notification of potential breaches by customers, and third-party incident response team reports. The key security proactive controls play in DLT systems are not sufficient to protect them from adversarial attacks. However, here we address intrusion discovery and incident response since contracting parties cannot expect that cybersecurity proactive controls can continuously provide perfect service security.

7.7. Technological Solutions

The success of an organization no longer depends solely on the strategic decisions made by its management team but also on the digitalization of its daily activities. Not only is technology helping reduce costs and enhance our productivity, but it is also destroying our competitive advantage. Marketing companies discuss what security breaches have recently affected our competitors because that provides them insight into our weaknesses. Customers and workers alike share their resentments on social media, warning anyone to do business with us. Employee spying has raised ethical concerns; so has the potential of our software to infringe on our rights or privacy. Every day, we hear news about companies or public bodies having their data encrypted. After doing so, hackers demand payment, promising to unencrypt it and secure the company against future attacks. Because the actions of individuals can affect the future of a country, national security may become the motivation for hacking. Cyber security is necessary and crucial for any organization to go worldwide, to transmit information and data securely across borders.

No information can be secured; we can only make it more difficult for attackers to access it. Enterprises should consider using encryption at rest, on the wire, and in use. Encryption software scrambles the data such that only parties with the decryption key can decode it. Encryption depends on two components -the encryption algorithm and the key–i.e., the method employed by the algorithm to encode the data. Medical organizations use public key cryptography for simple record security. Also known as asymmetric cryptography, this method allows two parties to communicate securely while using an easily-distributed public key. This public key encrypts the records, allowing anyone to send secure messages to the entity controlling the private key. However, the entity controlling the private key must decrypt these records with a private key, known only to itself. Thus, only the entity controlling the private key can read the encoded information.

7.7.1. Encryption Techniques

Data facilitating financial transactions is sensitive by nature, always accumulating attacks. Data transfers, in both directions, require particular care to avoid interception and misuse. A simple way to achieve that is through the use of encryption to make it unreadable while moving through the Internet. Cryptography is a science that attempts to mathematically achieve unbreakability and all the involved functions are implemented with an algorithm. It is worth mentioning that cryptography does not guarantee secrecy. Instead, it only allows the parties engaged in communication to ensure that the information it holds must not be revealed to a third party. For instance, cryptography may secure a debtor in the case the creditor discloses financial details to unauthorized third parties, who then use the data to damage its image, such as disseminating false information to third parties about the debtor defaulting.

Encryption contains two distinct functionalities: symmetric-cipher encryption and public-key encryption. The first one encrypts with the same key used in the decryption phase, therefore its applicability relies on the knowledge of a third party that needs to be overwritten with the secret key. This specificity reduces its application since the key must be supplied to every party engaged in the transaction. The second one differs by generating a pair of keys exclusive for a specific party, one private for decryption and one public for encryption made available to any third party wanting to establish contact. The public key encrypts and the private key decrypts messages. A big advantage in its application relies on the fact that a party that has entirely public keys of its business partners does not need to share any secret key, as required in the case of symmetric-key encryption. However, it is important to mention that the public key may only encrypt and not decrypt, so it is always recommended that sensitive data moving through the Internet be encrypted employing symmetric-key encryption.

7.7.2. Firewall and Intrusion Detection Systems

Firewall devices monitor and filter incoming and outgoing traffic on a network. Firewalls can be implemented as either hardware or software. For any organization, the firewall should be viewed as the first line of defense for their critical systems. However, firewalls cannot monitor every data packet and allow certain types of traffic that cannot be reviewed such as DNS or HTTP traffic. Some firewalls also rely on proxies to review this unexamined traffic; however, proxy implementations can be costly. Using an intelligent multi-tier architecture, we can avoid relying on a central monitoring point to review every data packet unlike the model used by traditional firewalls. We place certain firewalls in strategic locations to manipulate and modify data packets that are most vulnerable and use industry best practices to tailor these firewalls for the types of traffic

that are being transmitted through them. Firewalls can be custom-built entirely or modified to suit an organization's particular needs and requirements.

Intrusion detection systems are devices that monitor computer and network activities for malicious actions or policy violations and report these events. Traditional intrusion detection systems can be categorized as host-based intrusion detection systems and network-based intrusion detection systems. Host-based intrusion detection systems are software that are installed on each critical system and monitor for any unusual or suspicious activities on that specific device and send the logs to a specific designated location. Network-based intrusion detection systems are hardware devices that monitor the traffic on the entire network and send the logs to a specific designated location that is preferably protected with various levels of authentication or encryption. Detecting intrusions serves as a response strategy because it does not prevent an attack; it only creates awareness that there has been a possible breach of security or privacy.

7.8. Employee Training and Awareness

Cybersecurity is a rapidly evolving field. Employees represent the single most important asset of any organization. If they are not aware of cybersecurity threats and risks, all other security mechanisms will fail. Sensitive company information can be leaked, account access credentials compromised, and IT infrastructures damaged if employees act carelessly. Users' understanding of their role in keeping the organization secure is critical to success.

At the same time, holding users accountable for the compromises caused by a lack of awareness is akin to blaming a bank teller for falling victim to a phishing attack that gets their tellers to reveal their credentials. Miscreants are aware that their phishing attacks are their most effective means of getting access to secure functions and using them regularly. In a world where phishing attacks are often automated, organizations cannot expect employees to detect every such attack. Therefore, organizations must dedicate resources to ensure that employees understand the risks and threats associated with their use of machines, accounts, and other resources.

Many organizations offer training programs designed for practical daily operations. Enforced IT hygiene should be communicated to avoid bad blood between users and computer security staff who detect hygiene issues. Regular lunch-and-learn workshops allow employees to familiarize themselves with new technology and security policy issues. This can help to create a culture of community and inclusion. Certificate- or checkmark-based programs that allow employees to acquire security milestones can create better engagement. Organizations can also reward employees with free lunches or coffee for keeping account access through their cellular phones as clean as possible.

7.8.1. Importance of Cyber Hygiene

Cyber hygiene consists of practices that individuals or companies perform to maintain the health and hygiene of their systems, potentially reducing the risk of cyber breaches. These practices are similar to personal hygiene habits that we implement in our routines to protect and promote our health. Likewise, these actions will bolster your business's security by preventing expensive breaches that can be disastrous to your company, including data loss, reputation damage, and productivity loss. Cyber hygiene is important because it is a crucial part of the cybersecurity defense strategy for companies to defend against every form of cyber-attack. Traditionally, organizations prepare in advance their defenses to resist external threats or monitor actively the network to detect and react to breaches when they happen. However, in the last years, the sophistication level of attacks has grown significantly, making that strategy less effective. Therefore, companies are starting to implement additional strategies for increasing their security posture. Cyber hygiene products, services, and strategies strengthen your defenses and reduce the threat landscape, improving your cybersecurity posture. They can include: regular patches and upgrades, monitoring access, data loss prevention, identity controls, regulated and classified data, endpoint detection and response, data backup and disaster recovery, and physical access control. As time passes, we build more trust in others and the tools we use. We tend to be dangerous when using our phones or computers and connecting to public networks. But our minds get corrupted by some tools' convenience, forgetting to think twice before trusting a link, a message, or a Wi-Fi connection. Having concrete habits, provided by cyber hygiene methodology, help us signal these risks and better protect us, and the tools we use, from threats that believe they can exploit our unawareness.

7.8.2. Training Programs and Workshops

Employee training is the first line of defense against cyber threats and should be given the highest priority. It is also one of the simplest defenses to implement, offered internally or by third parties relatively cheaply. Employees are generally aware of physical threats to their workplaces but may not have considered data theft and cyber threats. Cyber incidents and loss of data are more likely to be caused by inadvertent mistakes than a specially designed cyber attack. These incidents can result in significant trust issues, especially in industries such as insurance, which is built on trust.

The insurance sector collects large volumes of sensitive personal data such as health, financial, and privacy information. This sector collects large amounts of data to assess risks and pay claims. Organizations in the insurance sector are prime targets for data breaches, theft, or loss due to the type and volume of sensitive information. The insurance sector must protect customer data and should take necessary measures to

prevent incidences of exposure. Employees should receive regular training to suit the audience within the organization. Staff responsible for managing networks and systems should undergo up-to-date technical training on secure environmental management and recognized security best practices. All employees should receive information and awareness training at induction and regularly thereafter, with shorter more frequent training sessions being preferred. Topics covered should include familiarization with and use of appropriate secure configuration procedures, and information handling and protection procedures. Training should also include the identification and use of appropriate risk mitigation procedures. Regular refresher training should be given on known threats both generic and recognized organization threats, and how to maintain security while continuing business. Advanced ongoing training should also be offered on the use of relevant monitoring and protection tools and general security awareness to more senior staff.

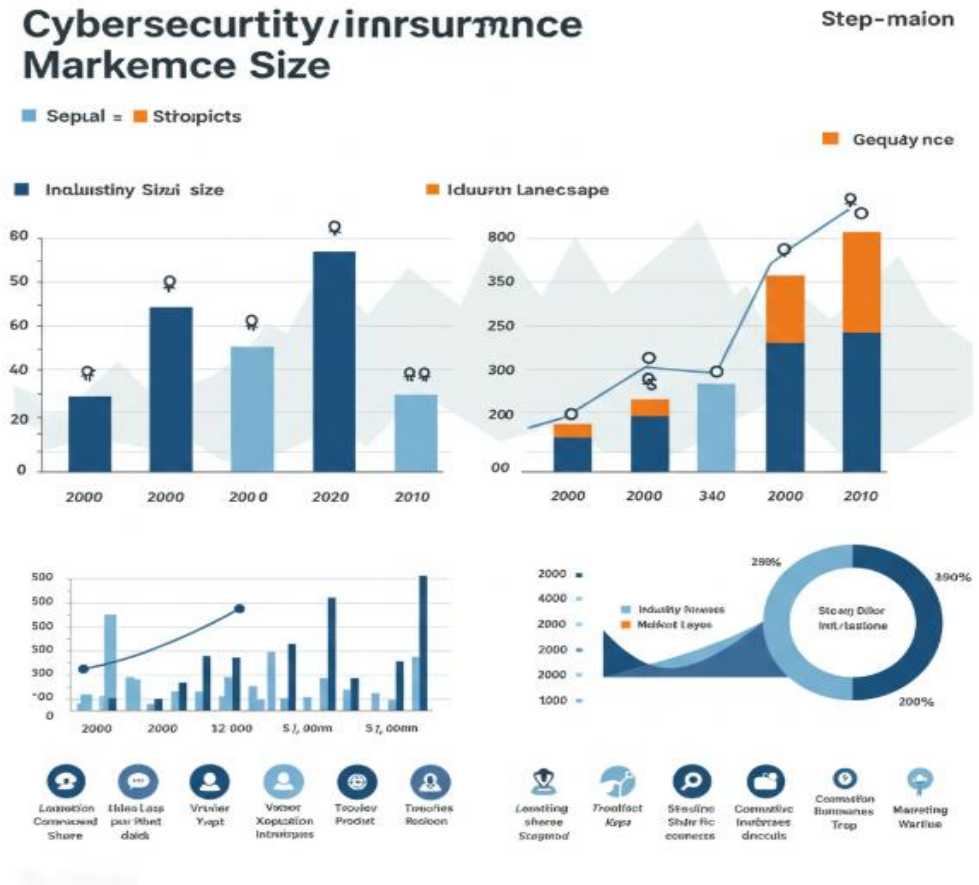

Fig 7 . 3 : Cybersecurity Insurance Market Size

7.9. Conclusion

As we have illustrated in this work, the reliance on digitalization in the insurance sector has been increasing in the past decade. Additionally, the acceleration of digital initiatives for customer engagement during the pandemic has created a new level of increased cyber threat to insurance organizations, particularly through the growth of ransomware. By becoming an essential part of the overall economy, the insurance sector is increasingly exposed to cyber risks. The security of an insurance organization's digital platform influences not only that organization but also the circle of customers and third-party partners regarding mitigating the cyber threat by preventing malicious actors from perpetrating data theft or theft by ransom. To ameliorate the increasing risk of cyber damage, the insurance sector as a whole must elevate its security game.

By doing so, insurance organizations can operate and offer insurance products, such as cyber coverage, that reside at the front lines of digital economy safety and security. This must occur before a pervasive network of ransomware actors causes overwhelming damage that makes information and cyber risk due diligence just another box to tick while a real security initiative is waiting to be implemented. A robust security posture by insurance organizations should include isolating sensitive data, incident detection, and response processes, account access controls, comprehensive risk assessment, and internal organization employee training and engagement that mold employees from the weakest link to the best asset against cyber threats. Creating an environment that will discourage actors from attacking digital platforms through seemingly insurmountable defenses is paramount for the sustainability of the insurance sector. The goal should be to reinforce the importance of investment in layered security specifically designed for insurance companies that can separate them from other organizations and industries, particularly from those that are traditionally viewed as being more exposed and easier to attack for ransomware actors.

7.9.1. Final Thoughts and Future Directions

Digital insurers must adopt creative secured management approaches along with robust data protection and regulated compliance. The insurance ecosystem must be a synergy of shared services and unbroken trust. The proposed model aims to create stable insurance digital platforms amid rising enterprise risk dividends that cyber threats can inflict on the insurance industry. The long-term objective is to develop the Digital Insurer, as a Unique Insurer, that surpasses the instinctive comparison of products and prices. Building agents and stakeholders' eco-trust through services and support must be the new era objective. There are many limitations in the study. The research is conceptual and qualitative. Expert validation should propel domain-empirical studies to enrich proposed models. A collaborative exploratory purpose would propel richer inputs to

validate insurers' objectives. Digital is a new world yet to be fully explored by humans. Security risks to stakeholders impact the global economy. The crisis has reinforced the necessity of an economy that cares for individuals, societies, and nature. Higher Cyber Security expenditures are needed. Cyber Security has long-term implications across investment horizons: individual, institutional, and societal needs. Providing platforms that are not only functional but also secure, trustworthy, and value-creating has lasting consequences on all agents who contribute to the Economy: households, corporations, and stakeholders. Income and price volatility considerations are missing in our research, as are capital market imperfections. Establishing and enforcing property rights associated with Cyber Insurance prices is outside our research limitations. Political participation by design creates promise through digital contracts property rights and credibility in digital services provided by Digital Insurers.

References

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things Security and Forensics: Challenges and Opportunities. Future Generation Computer Systems, 78, 544–546. https://doi.org/10.1016/j.future.2017.07.060

Almorsy, M., Grundy, J., & Müller, I. (2016). An Analysis of the Cloud Computing Security Problem. Future Generation Computer Systems, 62, 98–115. https://doi.org/10.1016/j.future.2015.09.006

Kshetri, N. (2017). 1 Cybersecurity and International Relations: The U.S. Engagement with China and Russia. Telecommunications Policy, 41(10), 1026–1041. https://doi.org/10.1016/j.telpol.2017.08.003

Fernandes, E., Jung, J., & Prakash, A. (2016). Security Analysis of Emerging Smart Home Applications. In: 2016 IEEE Symposium on Security and Privacy (SP), 636–654. https://doi.org/10.1109/SP.2016.44

Popovič, K., & Hocenski, Ž. (2010). Cloud Computing Security Issues and Challenges. In: Proceedings of the 33rd International Convention MIPRO, 344–349. https://doi.org/10.1109/MIPRO.2010.5533309