MSCA-RISE - Marie Skłodowska-Curie Research and Innovation Staff Exchange (RISE)

This project has received funding from the European Union's H2020-MSCA-RISE-2018 programme under grant agreement No 823997.

Security ECONomics service platform for smart security investments and cyber insurance pricing in the beyonD 2020 netwOrking era

SECONDO

WP5– Cyber Insurance and Smart Contracts

Deliverable D5.1 "Cyber Insurance Market, Attributes and Sources"

Editor(s):	CRO
Author(s):	Nikolaos Chondrogiannis (CRO), Aristeidis Farao (UPRC), Panagiotis Bountakas (UPRC)
Dissemination Level:	P
Type:	Report
Version:	1.4

Project Profile	
Contract Number	823997
Acronym	SECONDO
Title	Security ECONomics service platform for smart security investments and cyber insurance pricing in the beyonD 2020 netwOrking era
Start Date	Jan 1st, 2019
Duration	48 Months

Partners

University of Piraeus	University of Piraeus Research Center	Greece
UNIVERSITY OF SURREY	UNIVERSITY OF SURREY	United Kingdom
Τεχνολογικό Πανεπιστήμιο Κύπρου	Cyprus University of Technology	Cyprus
UBITECH ubiquitous solutions	UBITECH LIMITED	Cyprus
LS TECH	LSTech Espana	Spain
CROMAR INSURANCE BROKERS LTD	Cromar Insurance Brokers LTD	Greece
FOGUS INNOVATIONS & SERVICES	Fogus Innovations & Services P.C.	Greece
UNIVERSITY of GREENWICH	University of Greenwich	United Kingdom

Document History

VERSIONS

Version	Date	Author	Remarks
0.1	18/08/2020	CRO/UPRC	Table of contents
0.2	25/09/2020	CRO/UPRC	Participants and role
0.3	30/ 11/2020	CRO/UPRC	Coverages and commonalities among the proposal forms, analysis
0.4	19/12/2020	CRO/UPRC	Trends and issues
0.5	20/01/2020	CRO/UPRC	Trends and issues and SECONDO contributions
0.6	14/02/2020	CRO/UPRC	Trends and issues and SECONDO contributions
1.0	26/02/2020	CRO/UPRC	1st draft version
1.1	08/03/2021	UPRC	Review comments/Revision
1.2	12/03/2021	CRO/UPRC	Review comments/Revision
1.3	14/03/2021	CRO/UPRC	Review comments/Revision
1.4	15/02/2021	CRO/UPRC	Final version

Executive Summary

This document provides a comprehensive survey and analysis of the cyber insurance market and well-known insurance policies. It also presents common coverages from cyber insurance proposal forms of well-known insurance companies. In addition, the status and trends of the cyber insurance market are provided. Last, it presents major challenges of the cyber insurance market and how SECONDO will contribute towards addressing them.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

Cyber risks are an ever-increasing challenge of cyberspace that concerns a major share of the market playing a key role in the operations and decisions of organizations. The evolution of technology such as automation, integration of the Internet of Things (IoT), and Artificial Intelligence (AI), are accompanied by a wide range of threats and has led to sophisticated cyber-attacks. For years this has been a popular topic of discussion in academia and industry. Cyber-attacks became even more intense during the period pandemic when hit new record incidents. In a market that has not been matured without the necessary awareness cyber insurance companies are trying to redefine cyber insurance premiums. Malicious or intentional exposure of private data can potentially result in severe and lingering harm for the affected policyholders, as well as reputational damage to insurer sector participants. Cybersecurity incidents can have a great impact on insurers and harm the ability to conduct business, compromise the protection of commercial and personal data, and undermine confidence in the sector.

This section provides a brief overview of the cyber insurance market. Furthermore, provides a description of the participants in this market and the scope of the tasks carried out in this deliverable together with a summary of the future tasks and objectives to meet the proposed outcome of the project.

1.1 Role of this deliverable

The role of this deliverable is to provide a comprehensive survey and analysis of the cyber insurance market where the final and integrated SECONDO platform will be executed.

The present document has the following main purposes:

- To analyze the cyber insurance market.
- To analyze well-known cyber insurance policies.
- To identify cyber insurance trends.
- To identify critical attributes and parameters that influence cyber insurance.
- To recognize future cyber insurance market predictions.

1.2 Relationship to other deliverables

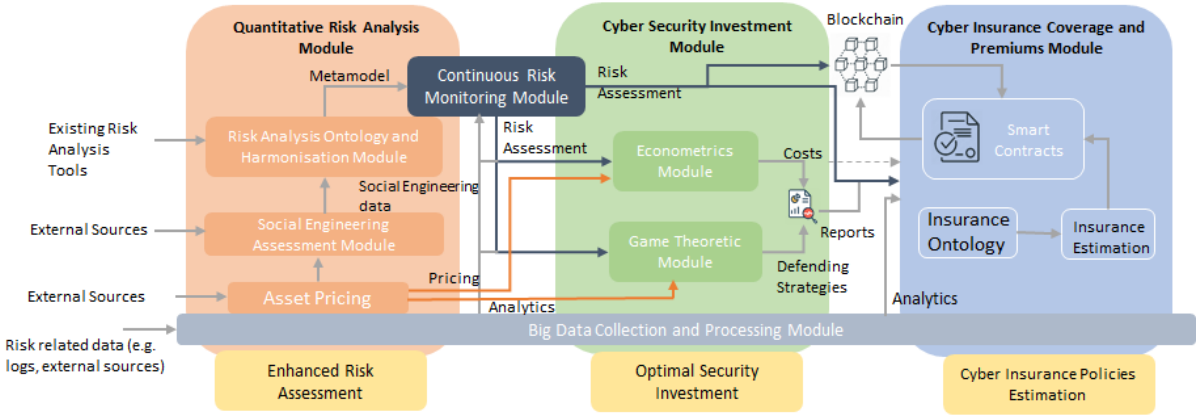

Figure 1 SECONDO Framework

This deliverable will be an input and a guidance for the rest upcoming deliverables of the SECONDO project since it analyses, in brief, the needs and issues of this market. Most of the upcoming deliverables are technical; however, their approach and output result should be tailored to the needs of this market.

- **D4.1: Econometrics:** The Econometrics Module (ECM) that provides estimates of all kinds of costs of potential attacks and costs, will respect the issues described in Section 5.
- **D4.2: Continuous Risk Monitoring and Blockchain:** The CRMM module will assess on a continuous basis the risk levels, including the performance of the implemented cybersecurity controls, will respect the issues in Section 5.
- **D4.3: Cyber Security Investments**: The CSIM module that will be responsible for inferring optimal investment plans will respect the presented issues in Section 5.
- **D5.2: Cyber Insurance Policy Ontology:** The Cyber Insurance Policy Ontology will follow the issues in Section 5 aiming to eliminate information asymmetry among the participants.
- **D5.3: Decision Support for Cyber Insurance:** The Cyber Insurance Coverage and Premiums Module (CICPM) will provide insurance exposure assessment and estimates insurance coverage and premiums based on the insurance policy of the underlying insurer, which will be modelled and incorporated using the developed cyber insurance ontology in respect to the issues of Section 5 achieving better prices and creating a more antagonistic market.

1.3 Structure of the document

The rest of the deliverables is structured as follows. Section 2 analyses cyber insurance, providing an in-depth analysis of the participants as well as the description of the insurance process. Next, Section 3 presents the common cyber coverages provided by well-known insurance companies. Section 4 provides a general description of the current trends that follow the cyber insurance market together with predictions for the near future. Section 5 presents the issues of the cyber insurance market, while Section 6 proves how the SECONDO platform can cover the gap created from these issues. Finally, Section 7 concludes the deliverables.

2 Cyber Insurance background

Concern over cybersecurity is growing across all sectors of the global economy, as cyber risks have grown, and cyber criminals have become increasingly sophisticated. For insurers, cybersecurity incidents can harm the ability to conduct business, compromise the protection of commercial and personal data, and undermine confidence in the sector.

2.1 Cyber Insurance participants

This section presents that participants who take part in the cyber insurance market. They are the following: i) Insure; ii) Insured; iii) Agent and iv) Broker. We will analyse them below.

2.1.1 Insurer

Over the years the need for more sophisticated services and specialized insurers becomes more and more necessary in the field of cyber security. The role of insurers has become more significant and has evolved to respond to the current needs of today's market. A characteristic of an insurer is that can adapt and provide tailor-made solutions in individuals and businesses, offering support when an event occurs. This applies particularly in today's needs where individuals and organizations are struggling to protect their privacy from cyber threats in terms of cybersecurity. It is observed that through years the cyber-attacks are becoming more complex and sophisticated.

The substance of insurance is to secure individuals and organizations from risks. This is done when individuals and businesses buy a premium from an insurance company to be insured in case of a catastrophic exposure. Insurance provides economic protection from identified risks occurring or discovered within a specified period. Holding a cyber premium, a policyholder can mitigate the risk by insuring business as the revenue - premium payments by policyholders - are received before or during the coverage period [1]. One of the main purposes of an insurer is to aware customers about the cyber risks and outcomes of a potential incident. Insurers have an important role in increasing cyber resilience and competitiveness in the EU. Insurers can ensure the smooth running of businesses but enable them to regroup after a cyber-attack. It is also worth mentioning that insurers can raise the awareness organizations about the dangers that are hidden in cyberspace and how they can be exposed, offering effective protection against them with cyber premiums. Risk mitigation, avoidance, and prevention are also an integral part of insurers to help companies and individuals to manage cyber risks.

Insurers can offer premiums that can cover a variety of cyber risks and incidents, such as phishing, data breaches, or malware that can affect companies and individuals. It can provide first-party coverages, such as damage on digital assets, business interruption, and incident response costs, as well as third-party coverage, such as privacy and confidentiality-related liabilities. Moreover, insurers provide policy holders with premiums and with the element of risk assessment, in case they fall victim to a cyber threat, providing technical, legal support in case of an incident. There is quite a lot of variation between the contracts, and this always depends on the needs of individuals or organizations. Also, it depends on the need for insurance coverage as well as the type and level of risks that will be exposed. Insurers offer cyber insurance policies as part of a contract or as a standalone product [2].

Nowadays, Insurance companies, not only aim to provide services insuring individuals and companies

but also to address a more complex situation involving intangible threats such as reputation to protect from risk, their client's sensitive data. Based on the above and the current trend, insurance companies offer cyber insurance premiums including coverages for related cyber crises including but not limited to business interruption.

2.1.2 Insured

Insured is a person whose assets (tangible and intangible assets) are protected by an insurance policy; moreover, he is a person who contracts for an insurance policy that indemnifies him against loss. In terms of cyber insurance individuals and organizations can benefit as cyber incidents can evoke cyber risks. Aftermaths of a cyber threat may have a negative impact on individuals and businesses, including the loss of customers and revenue. Cyber insurance policies may change as an impact of the continuously changing market. Insurers nowadays are facing many challenges in the insurance industry such as, the need to find a trusted advisor, to find the proper insurance program, to find a broker or agent who addresses their specific and special insurance needs, a competitive insurance program in comparatively the current market environment and to find a tailor-made contract in their needs.

2.1.3 Agent

An insurance agent is a licensed person who has an important role to achieve an agreement and to conduct business on behalf of insurance companies. He is the professional who has the necessary knowledge needed to transmit the multifarious to the prospective clients. He is the intermediary who has undertaken the difficult role of approaching the client, informing him about the offered products of the insurance company, convincing him to buy them, and most important and the most difficult part is to acquire trust and become the person who will be interested in satisfying him, regarding the agreed claim that insured has. However, the insurance agent is the one who must study the financial conjunctions, analyse them, predict the changes that affect the interested parties by all factors such as consumers, investors, those who are interested in savings plans, and all those who are interested to be insured.

The role of an agent can be differentiated regarding the market. In some can work as “independent” and can collaborate with more than one company and in others, operates exclusively – either representing a single insurance company in one geographic area or selling a single line of business for each of several companies. There are different forms in which can operate an agent and are entitled as independent, exclusive, insurer-employed, and self-employed [3].

Agents are the legal representatives of clients with the right to perform certain acts on behalf of the insurers they represent, such as to bind coverage. Another definition that is used to describe an agent is a professional who advises clients to choose insurance policies that are suitable for their needs. Also, is referred to as a person who sells insurance products from the insurance company who work. Insurance agents are hired from a company or an organization to find clients and sell only their products. Agents are not interested to compare prices or characteristics with other products/services that exist in the market. On the contrary brokers can compare products and prices from several insurance providers. Moreover, in the category in which belong, the independent agents can collaborate with different companies similarly to insurance brokers. Also, there are companies where

they collaborate only with agents, so their products do not appear among the products offered by brokers.

An insurance agent should be characterized by experience but also by specialized knowledge that includes all the operations of the company in which he works as well as the products and services he offers. The basic condition is the theoretical knowledge, he must constantly learn new techniques (e.g., through seminars, big economic-social books, and magazines) to understand the market and the competition. Another important piece of information is that agents must keep a record of clients that includes marital status, copies of contracts, copies of plans, circulars, correspondence, client payments.

The agent is the one who determines the terms of a contract and takes over the responsibilities and determines the terms of insurance and invoicing. Moreover, is responsible to determine the number of reserves and outstanding losses. Additionally, must determine the premium according to the terms of the agreement. During the insurance contract, he must be ready to fulfil his insurance duties in accordance with the terms agreed in the insurance policy. Insurance agents must develop relationships with prospective clients through networking and referrals. They crate the right basis to build strong relationships with customers and to achieve fruitful communication between stakeholders, thus building long-term relationships. Finally, the reputation of an insurance agent depends on the reliability of contact when a client needs to file a claim or increase their coverage due to major life events.

2.1.4 Broker

The term “brokers” has been described with many definitions; Ronald Burt (1992, 2001) defines brokers as individuals who make possible a bridge between two discrete networks. Robert Chaskin and associates (2001) define “organizational brokers” as community-building organizations that tie separate organizations to one another to accomplish local neighbourhood tasks and build community capacity. While Burt’s brokers tie individuals to other individuals, and Chaskin and colleagues’ brokers tie organizations to other organizations, resource brokers, in this study, tie individuals to organizations, and, importantly, transfer resources to the individual [4]. A broker is also referred to as an individual or a company who does transactions on their behalf, providing to consumers the best services or products with a charge of a commission. Moreover, a professional who searches for more suitable or creates tailor maid insurance policy to meet the consumer’s needs.

In addition, brokers organize and execute financial transactions on behalf of their respective clients for categories such as assets stocks, forex, real estate, and insurance. For the orders he executes, the customers are charged with a commission according to the agreement of the contract. A broker can have an advising role on buying or selling products as some can provide their customers with market data analytics to help them make the right decision. The broker may be full-time or only for executions. To do the above he must be certified to provide the appropriate advice as well as the client's permission to perform any action. There are some types of brokers which we will analyse below and act as a facilitator between clients and another party while they operate differently from each other. Some manage portfolios and offer advice while others are only to *execute* as: i) Stock Broker; ii) Forex Broker; iii) Full - Service Broker; iv) Discount Broker; v) Commodity Broker; vi) Insurance Broker; vii)

Real Estate Broker and viii) cyber broker. However, we will focus and analyse only the cyber broker since this actor is the one who plays the mediator's role among the insurance companies and insureds.

- **Cyber Insurance Broker**
  Cyber insurance brokers are intermediaries who do market research to bring the best contracts to their clients. Professionals belonging to this category help their clients by cultivating awareness of the dangers in cyberspace, with products that offer sufficient coverage for the needs of everyone. This translates into an offer of complete insurance packages but also as covering specific needs of each customer. Moreover, a broker is the mediator who will deliver the information which is necessary to serve the insurance company and the insured (or prospective insured). Hence, brokers are trusted consultants but in terms of Cyber Insurance but do not specialize in cyber security. Their role is to do market research, to be informed, to understand the special needs of each customer to offer insurance premiums on the most favourable terms to their customers. They also need to be informed and especially regarding the cybersecurity part to guide and advise their clients with tactics to avoid threats and manage threats in the workplace. Brokers are professionals in the field who are properly trained and licensed to offer their services. A company will never be able to protect itself 100% from a cyber-attack. With the development of technology and new types of cyber-attacks, brokers aim at providing the required and satisfactory insurance premiums for their clients (prospective insured) and insurance in software and hardware. Also, they must deal with threats and insure more complicated assets, for example the theft of personal data and defamation [5], [6]. Having a broad knowledge of the insurance market including products, providers' prices as well as a strong sense of the needs of insurance buyers, intermediaries have a unique role in market viability.

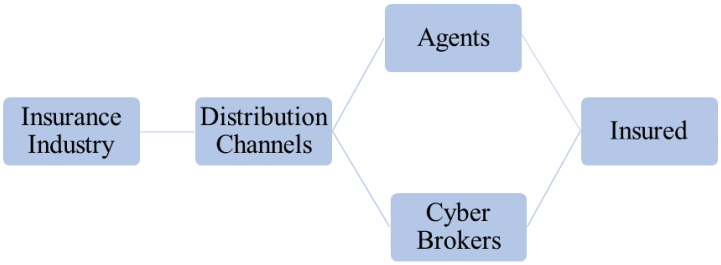

Figure 2 Cyber insurance ecosystem

2.2 Insurance process

Marotta et. al. in [7] analysed the insurance process in the following three main pillars: i) **Risk identification**; ii) **Risk analysis** and finally iii) **Establishing contract**. First and foremost, an external authority (or insurance company's representative) identifies the main parameters of risk. Once it is successfully completed, the risk is analysed by determining the probability of occurrence of each threat, the probability of being compromised due to the corresponding threat and finally the possible impact of an incident. After completing this important step, the broker and the insurance company

specify the coverages and the premium. After signing the contract, and in case an incident has occurred during the contractual period, the broker may make a claim to the insurance company to cover the losses. The process could be as follows:

1. **Risk Identification**: Risk identification is the process of determining risks that could potentially prevent the program, enterprise, or investment from achieving its objectives. It includes documenting and communicating the concern.
    a. **Asset Identification**: Asset identification is the use of attributes and methods to uniquely identify an asset, allows for correlation of data across multiple sources, reporting of asset information across different organizations and databases, targeted actions against specific assets, and usage of asset data in other business processes [8], [9]
    b. **Threat Identification**: Risk identification is the process of determining risks that could potentially prevent the program, enterprise, or investment from achieving its objectives. It includes documenting and communicating the concern.
    c. **Security/Vulnerability Identification**: Security/vulnerability identification is a review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities [10], assigns severity levels to those vulnerabilities [11], and recommends remediation or mitigation [11], if and whenever needed.
2. **Risk Analysis**: The risk analysis involves a review of the data gathered during the phase of risk identification (it is the previously mentioned phase) and an analysis of the resulting risk to the organization. During this phase, the security risk assessment team determines asset values, system criticality, likely threats, and the existence of vulnerabilities based on the data gathered. Furthermore, the team must calculate the risk to the organization for each threat/vulnerability pair. The calculation and presentation of these risks can vary greatly, depending on the security risk assessment method being used.
    a. **Likelihood Determination**: This phase determines the likelihood that the threat event will occur and result in adverse impacts.
    b. **Impact Determination**: This phase determines the adverse impact from a successful threat event.
    c. **Risk Estimation**: This is the final phase and is responsible to determine the level of risk as a combination of likelihood and impact. The most well-known equation to calculate the risk is the following [12].

$$Risk = Assets \times Threats \times Vulnerability$$

3. **Establish Contract**: During this phase, the insurance company and the prospective insured establish the contract, its cost and determine the coverages and the exclusion. Also, the claim handling is part of this phase; however, it is optional since it will occur only if an incident successfully occurs.
    a. **Coverage Specification**: This is a detailed description of the coverage types, amounts, and policy provisions submitted to an insurance company to use in preparing a

proposal. Insurance specifications also typically include the underwriting data the insurance company will need to price the required coverages.

b. **Premium Estimation**: Is the estimation of a premium cost that an insurance company provides to a prospective policyholder.
c. **Write and Sign Contract**: The contract is written and signed by the insured who becomes the legal policyholder.
d. **Claim Handling (optional):** Once a claim has been reported (due to an incident), then an investigation will start. Then the policy will be reviewed to be determined what is covered and what is excluded. Then, the damage evaluation is conducted to accurately evaluate the extent of the damage. Once it is done, the payment is arranged.

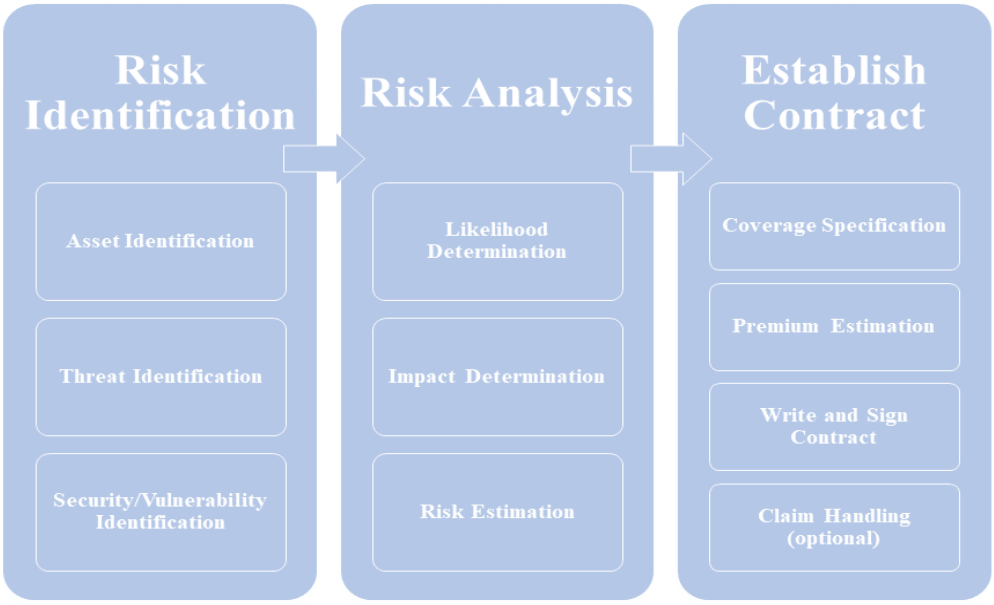

Figure 3 Insurance process flow

3 Existing status of the market

3.1 Cyber insurance proposal forms

Cyber Insurance proposal forms contain coverages that can be categorized in **first-party coverages** and **third-party coverages**.

First-party cyber liability insurance provides financial assistance to mitigate the impact of data breaches and cyberattacks at an organization. This policy is crucial for businesses that store sensitive client or customer information online, such as credit card numbers or social security numbers. Being more specific, it covers the costs of:

- Providing credit monitoring
- Executing PR and reputation management campaigns
- Other recovery activities

On the other hand, third-party coverage can cover expenses for businesses responsible for clients' online security and data. If an IT company's client experiences a ransomware attack or data breach and sues the IT business, third-party cyber insurance can pay the necessary legal expenses to defend the business in court. Third-party cyber insurance is often included in a tech professional's errors and omissions insurance policy. This package is called technology errors and omissions insurance. It helps pay for lawsuits when a business – either because of its actions or lack of action – is sued for causing a data breach or another mistake or oversight.

Currently, there are many available cyber insurance proposal forms that are provided from many different insurance companies (also known as insurers). In this deliverable we focus on cyber insurances, which are delivered by many insurance companies from all over the world including Europe, United States of America, India, and Asia, aiming to present the differences on the offered covered liabilities. To conduct this research, we focused on available for free insurance policies from globally well-known insurance companies, who are globally located. We have investigated thirteen insurance companies which had available for free cyber insurance proposals forms. The investigated policies are from 2018 until 2020. We note that we avoid naming the investigated insurance companies. Each cyber insurance policy is unique. However, all these have common covered liabilities. Woods et. al. [13] investigated cyber insurance proposal forms and presented the most common coverages in 2017. We can observe that the same trend on coverages still exists; however, the current trend has enriched the common coverages. The common coverages are analysed below.

Table 1 summarizes the comparison of the investigated cyber insurance proposal forms; the comparison is based on the following signs: ✔, –, (✔), (–).

- The ✔ sign declares that the respective coverage is provided.
- The - sign presents that the respective coverage is not covered by the corresponding proposal form.
- When these two signs above are put into parentheses, (✔) and (-) it means that the respective coverage does not include all the details needed, and we had to make assumptions to conclude.

Technology wrongful act: This coverage involves any act that fails to render a technology service or technology products so that these are not able to serve their designed purpose. Technology products include tangible assets, e.g., telecommunications hardware, while technology service includes intangible assets, e.g., computer networking. It could get triggered by an act of error, omission, neglect, negligent misrepresentation, or breach of duty.

Professional wrongful act: This coverage involves any act that fails to render a professional service so that it is not able to deliver its planned purpose. Professional services include services related to accounting, law, management consulting, which are outsourced by a company to a third-party organization. It could get triggered by an act of error, omission, neglect, negligent misrepresentation, or breach of duty.

Media wrongful act: This coverage involves any expenses done due to a range of media actions that are committed in gathering, communicating, reproducing, publishing, disseminating, displaying,

releasing, transmitting, or disclosing Media Content via any Computer System of Insured. A small sample of media actions are the unauthorized use of copyright, title, trademark or service name, a violation of an individual's right of privacy or publicity and the defamation, libel, slander, trade libel or other tort related to disparagement or harm to the reputation or character of any entity of Insured Company.

Privacy and security wrongful act: This coverage involves any loss, theft, or failure to protect, or unauthorized acquisition of personally identifiable information, protected health information, or confidential business information. Moreover, it includes violation of any law, statute or regulation governing the authenticity, availability, confidentiality, storage, control, disclosure, integrity, or use of personally identifiable information or protected health information. Also, it covers violation of a data breach reporting requirement, failure to reasonably implement privacy or security practices required by law or regulations. In addition, it includes failure to prevent a cyber security breach that results in: the inability of an authorized user to gain access to the network; the malicious addition, alteration, copy, destruction, deletion, disclosure, damage, removal, or theft of data residing on the network; or the transmission of malware from the network to third parties. Finally, it covers failure to comply with the insured company's privacy policy and/or privacy notice.

Business regulatory defence, awards, and fines: This offers coverage against regulatory fines and penalties and/or regulatory compensatory awards incurred in privacy regulatory proceedings/investigations brought by federal, state, or local governmental agencies.

Business interruption and extra expenses: This coverage includes any expenses incurred by the insured when a computer system or service of the insured fails or degrades or is in partial or total interruption. The expenses are spent during the period of restoration that begins after the time of interruption and ends on the earlier of the date when the computer system or service is restored with reasonable speed to the same condition, functionality and level of service that existed prior the interruption.

Data recovery: This coverage involves any expenses incurred by insured to replace, recreate, restore, or repair any damaged or destroyed computer programs, software, or electronic data to substantially the form in which it existed to immediately prior to a cyber security breach. Expenses also include any act for determination whether damaged or destroyed computer programs, software, or electronic data of insured needs data recovery.

Cyber extortion/Ransomware: This coverage protects against any threat that demands payment in consideration for the elimination, mitigation, or removal of the threat. The intentions of threats are network disruption, damage of data stored on the network, refusal to return data stolen, prevention of access to the network or data by using encryption and withholding the decryption key. The actors of threats are usually a third party or an employee of the insured company who deliberately act outside the scope of employment.

Data breach response and crisis management coverage: This coverage involves any expenses incurred by insured to manage a crisis caused by any cyber security breach and respond to any data breach. These expenses can come from a rich basket of actions made by a pre-approved panel of

breach response vendors. Actions with direct impact for insured are to perform computer forensics determining the existence, cause and scope of a data breach or cyber security breach, to operate a call centre to manage data breach inquiries and to minimize reputational harm by hiring a public relations or crisis communications firm. Actions which are addressed to individuals whose personally identifiable information was breached are to notify them and to provide credit or identity monitoring, identity protection, restoration services and any similar services.

Loss of digital asset: This coverage involves any loss incurred as a direct result of damage, alteration, corruption, distortion, theft, misuse, or destruction of insured's digital assets. Digital assets include computer programs and electronic data that exist in a computer system. Computer hardware is excluded.

Cyber terrorism: This coverage involves any income loss and any expenses incurred by insured the period of restoration after an act of terrorism. An act of terrorism is any act of any person or group(s) of persons, committed for ideological, political, religious, or similar purposes to influence any government and frighten the public or any section of the public. The terrorists act alone, but most of the time they act in connection with any organization(s) or governments.

Dependent business interruption: This coverage involves any cyber business interruption event caused by an event that occurred at a third part but directly affects the insured.

Pre-claim assistance: This is an assistance including but not limited to payments regarding legal, forensics, IT support to help an insured to mitigate or prevent a claim or incident before it occurs. Moreover, it contains access to a 24/7 support team.

PCI DSS assessment: This coverage involves any costs that an insured need to pay to his bank due to PCI-Fines and PCI-DSS Assessments. In this case the insured is a company which accepts credit cards and is obliged to protect payment card data, signing a Merchant Services Agreement with its bank. If a security breach occurs and the breach is related with payment card data, then the company is non-compliant with rules and the company may be subject to PCI-DSS fines and PCI-DSS Assessments.

Cyber-crime: This coverage involves any act that fails to prevent or hinder attacks which were intended to harm insured's computer system. These attacks are denial of service, malicious code, unauthorized access, and unauthorized use. It could get triggered by an act of mistake, negligent error, or omission in the operation of insured's computer system or handling of insured's digital assets. The act is triggered by insured's employee or outsourced IT service provider of insured or by any third-party independent contractor that provides business process outsourcing services e.g., call centre services, fulfilment services and logistical support.

Natural peril: This coverage involves any loss arising out of a natural peril, such as fire, including but not limited to fire, wind, water, flood, subsidence, or earthquake, that causes damages to computer hardware, data centre or basic infrastructure of the insured.

Table 1 Coverages provided by cyber insurance policy forms.

Coverages	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
Technology wrongful act	✓	✓	✓	-	-	✓	✓	(-)	✓	✓	(✓)	(-)	(-)
Professional services wrongful act	✓	✓	✓	-	-	✓	✓	(-)	✓	✓	(✓)	(-)	(-)
Media wrongful act	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	(✓)
privacy and security wrongful act	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
privacy regulatory defence, awards and fines	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Business interruption and extra expenses	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data Recovery	✓	-	✓	-	✓	✓	-	✓	(-)	✓	✓	✓	✓
Cyber Extortion	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ransomware	✓	-	✓	-	✓	✓	✓	(✓)	(✓)	✓	✓	(✓)	✓
Data breach response and crisis management coverage	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application of coverage	✓	-	-	✓	✓	(-)	(-)	(-)	(-)	✓	(-)	(-)	(-)
Loss of digital Assets	-	✓	-	-	✓	✓	-	✓	✓	✓	✓	(✓)	(✓)
Cyber terrosrism	-	✓	-	-	-	-	-	✓	✓	(-)	-	-	-

Dependent Business Interruption	-	-	✓	✓	-	✓	✓	(-)	✓	(✓)	✓	(✓)★	-
Pre-claim assistance	-	-	✓	-	-	✓	-	✓	(✓)	(-)	-	-	-
PCI DSS assessment	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓
Cyber Crime	-	-	(-)	✓	✓	-	✓	✓	✓	✓	✓	✓	-
Natural peril	-	✓	(-)	-	-	-	(-)	(-)	(-)	-	(-)	-	(-)
★ *unless provider is hosting hardware or software that is owned by the Insured*													

Table 2 summarizes the comparison of the investigated cyber insurance proposal forms and presents the events that each insurance company understands as business interruption; the comparison is based on the following signs: ✓, –, (✓), (–).

- The ✓ sign declares that the respective coverage is provided.
- The - sign presents that the respective coverage is not covered by the corresponding proposal form.
- When these two signs above are put into parentheses, (✓) and (-) it means that the respective coverage does not include all the details needed, and we had to make assumptions to come to a conclusion.

Table 2 Cybersecurity events considered as business interruption events.

Business Interruption	1	2	3	4	5	6	7	8	9	10	11	12
Distributed denial of service (DDoS) attack	-	-	-	-	✓	-	✓	-	-	-	-	-
Malware	✓	(✓)	(-)	(✓)	✓	(-)	-	(-)	(✓)	-	-	✓
Denial of service (DoS)	✓	✓	✓	✓	✓	(-)	-	✓	✓	✓	✓	✓

Malicious code	-	✓	✓	✓	✓	(-)	✓	✓	✓	-	-	✓
virus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
Unauthorized use of a Computer System	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
Unauthorized access to a Computer System	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
Unauthorized use of data assets	-	✓	✓	✓	-	✓	(✓)	✓	✓	✓	✓	-
Unauthorized access to data assets	-	✓	✓	✓	-	✓	(✓)	✓	✓	✓	✓	-
Worms	✓	✓	-	✓	-	(-)	✓	✓	✓	✓	-	-
Trojan horses	✓	✓	-	✓	-	(-)	✓	✓	✓	✓	-	-
Spyware	✓	✓	-	✓	-	(-)	✓	✓	✓	-	-	-
Adware	✓	-	-	-	-	(-)	-	✓	-	-	-	-
Zero-day	✓	-	-	-	-	(-)	-	-	-	-	-	-
Hacker attacks	✓	-	-	-	-	(-)	-	-	-	-	-	-
Logic bombs		✓	-	✓	-	(-)	✓	✓	✓	✓	-	-
Spider ware	-	-	-	-	-	-	✓		-	-	-	-

Past or present employee	✓★	✓	(-)	✓★★	-	✓	✓	✓★	-	(-)	-	-
Brute force attack	-	-	-	-	-	-	✓	-	-	✓	-	-
Phishing	-	-	-	-	-	-	✓	-	-	✓	-	-
★ No Executive officers												
★★ If stolen credentials are used												

From Table 2, we can observe that each insurance company identifies the business interruption as the result that occurs from different cyber security events. The most common incidents are the interruption due to a virus, unauthorized use, and access of a computer system. However, the most interesting result that we can deduct from this table iss that the majority of the investigated insurance companies do not cover business interruption that is initiated through a phishing attack. A research [22] has shown that spam/phishing filtering software only has a success rate of 93%. Given the sheer quantity of phishing emails in circulation at present, this gap of 7% ensures that a significant number of phishing emails end up in the inbox along with legitimate e-mail - and this is where the danger lies. 1 in every 1,846 e-mails sent globally is a phishing email. Moreover, research has shown that the cost of a cyber-attack to an organisation is proportionate to the number of employees, with the average cost estimated at $395 USD Per Employee – Per Attack [14]. We must note that the aforementioned comparisons are based on the proposal forms of the insurance companies; these can be configured based on each insured's demands.

Another interesting issue is that fines and penalties may be imposed by a variety of regulatory authorities for breaches of obligations to shareholders, employees and/or consumers. The ability of affected policyholders to be reimbursed by insurance for fines and penalties imposed depends on the terms and conditions of the coverage, the authority imposing the fine and the type of fine (civil/administrative or criminal and whether punitive or compensatory), the specific jurisdiction where the fine is being imposed and the nature of the act being penalised –which could lead to uncertainty regarding which fines and penalties are likely to be reimbursed under an insurance policy. In most countries, the vast majority of cyber insurance policies offer some coverages for fines and penalties [15].

4 Current trends and future prediction in the market

Cyber insurance is still in its infancy although cyber insurance services have been available for a few years. It is a sector that is in a stage of maturation and evolution as it tries to respond to the needs of the market but also to keep pace with the evolution of technology. Specialized coverage against

computer crime first appeared in the late 1970s while at the same time a security research was published on computer crimes [16]. Prior to the early 1990s, there was little demand from the consumer community for creating insurance services that would protect against network security breaches or other IT-related problems. The growing demand for insurance services became strong in the early 2000s when wide known companies like eBay, Amazon.com, CNN.com saw their websites crash for several hours after being attacked by hackers with a cost of 1.2 Billion [7]. After breaches, the market needed cyber insurance premiums to be covered from future cyber-attacks. Hence turned organizations to see the gap in the market, recognize market constraints, cover cyber risk issues, sell products/services, and fill the gap in the market. In 1998, the first companies appeared to focus on the cyber insurance market with premiums that covered the needs for hardware and software insurance as well as data loss from attacks, malware, data theft, etc. following specialized policies with a flaw of high-cost services.

Companies have developed two different ways of insuring (First-party and Third-party) in order to meet the cyber needs of both companies that work in IT and other types of companies. First-party coverage includes loss or damage to digital assets, business interruption, cyber extortion, theft of money, and digital assets. Common third-party coverage may include security and privacy breaches costs, computer forensics investigation, customer notification costs, multimedia liability, loss of third-party data, third-party contractual indemnification. Considering the above, the market is still in its infancy. CIAB [17] and PwC [18] characterize the current state of cyber insurance as a soft market with excess capacity due to an influx of new insurers entering the market.

“The demand for cyber insurance is growing, insurers are wary of expanding coverage due to lack of credible data, interdependent security, asymmetric information issues such as adverse selection and moral hazard, and the potential for catastrophic aggregate losses in the face of correlated exposures among policyholders. The result leads to cyber insurance policies with gaps in coverages and lower limits that do not indemnify insureds for many cyber losses” [19] [20].

In 2020, when the coronavirus hearsay started, there was a sharp increase in the contracts for protection against cyber-attacks. According to a report by Aon, insurance contributions have increased since 2012 by about 30%. In 2020 it is occurred an increase of 50% compared to 2019. As the cyber threat evolves and becomes more sophisticated as well as grows the demand for cyber insurance. Lloyd’s Class of Business team estimated that the global cyber market was worth between $3 billion and $3.5 billion during the year 2017 [21]. By 2020, some analysts estimate it could be worth $7.5 billion [22]. Something that was achieved since the global cyber insurance market in 2020 was $7.9 billion [23]. This value is estimated to become $20.4 billion by 2025. The factors that influenced this increase are:

- The market is at an early stage while at the same time is going through a transitional period increasing premium prices.
- Companies that are already familiar with cybersecurity, are increasing their services to respond more accurately to cyber risks.

- Increased awareness of cybersecurity leads to a larger influx of new customers throughout the year, in all industries.

We observe that with the current market situation there are opportunities for growth and as more entities claim part of the market, the greater mobilization succeeded, resulting in higher security awareness about threats and the supply of innovative products. Of course, there is a need from all sides to deepen understanding of cyber risk as the core challenges for the Industry increase [6]. The market size of cyber insurance has been increased frequently and will follow this trajectory as it is predicted. Both Small-medium-enterprises (also known as SMEs), as well as large organizations, invest in this market by buying insurance.

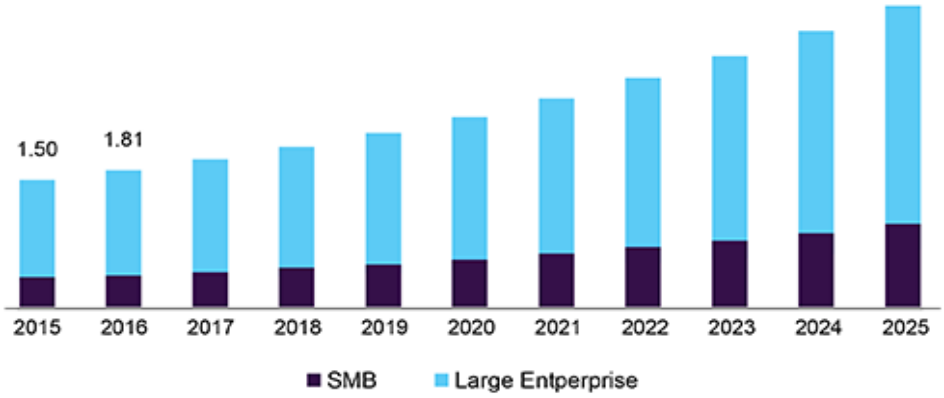

Figure 4 Cyber insurance market size by organization, 2015-2021 (USD Billion) [24]

The cyber insurance trends are totally affected from the COVID-19 existence. Some employees still work remotely, for instance Facebook allows its employees to work home permanently [25], while many companies go permanently digital. However, this alternation of the work environment - being remote- bears an expansion of cyber-attacks that have accompanied the "work anywhere" operating models. To take on the new cyber security challenges of this virtual working environment, organizations must understand the changes in their cyber security risk profile and revamp their strategies, training, and exercises to address these changes [26]. Five key factors drive the cyber security risk implications in this new, likely semi remote, working environment. Organizations should keep these factors in mind when defining how to adjust their cyber security risk programs: i) *an increasing number of cyber-attacks*: from the beginning of COVID-19 outbreak the cyber-attack incidents have been skyrocketed since hackers have exploited a greater number of weakly protected back doors into corporate systems (IC3 announced that receives 3K-4K cyber security complaints every day [27]; ii) *changing attack surfaces*: the aforementioned change to new teleworking infrastructure and processes may lead to the undetected exploitation of vulnerabilities in existing remote work technologies. A joint advisory published (April 8, 2020) by the UK's National Cyber Security Centre (NCSC) and US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) shows that cyber criminals and advanced persistent threat (APT) groups are targeting

individuals and organizations with a range of ransomware and malware. In addition, cyber risks via business partners and third parties are increasing as well; iii) Distracted workforces: A whopping number of successful cyber-attacks are caused by human error, while 95% of cybersecurity breaches are due to human error and Cyber-criminals will infiltrate your company through its weakest link, which is almost never in the IT department. Increasingly preoccupied by greater personal and financial stress at home, employees are more vulnerable to cyber threats and “social engineering” cyber-attacks designed to trick them into revealing sensitive information; iv) *unanticipated staff shortages*: During the COVID-19 outbreak many employees took time off for health issues who belong to various departments; however, this trend decreased the productivity among the industries including processes related to cyber security and v) *multi-stress environment:* Security teams are operating in an unprecedented environment in which multiple crises are constantly arising. We can observe that as organizations move to new ways of working (teleworking), the resulting changes to the company’s cyber security risk profiles must be repeatedly assessed and monitored so that they can be actively managed, prioritized, and mitigated. Organizations should execute some necessary steps like revising the existing cyber risk guidelines, requirements, and controls on how employees access data and communicate with a company’s network from the new remote office.

Cybercriminals continue to exploit the confusion caused by the COVID - 19 pandemic. Cyber risks are on the rise as technology and insurance have significant leading roles in the market. The rapid increase in cyber-attacks has frozen the market. Insureds and insurance companies are in a state of reconstruction, considering how cybersecurity is being modelled. The change plan includes fine tunings of existing insurance models, aligning with short tail insurance. With this change, the insurance companies aim to deal with the rapid occurrence of damages caused by cyber-attacks. With the changes that the current situation has brought, insurers are redefining their pricing policy as they consider how the cyber premium pricing models should be developed.

Cybersecurity is becoming more as a necessity, offering solutions, as the consequences of the attacks are becoming more noticeable. Based on the needs, alternative cyber solutions are expected to emerge as mainstream options in the future, providing solutions where other lines of insurance have retracted from the emerging exposure. The most common types of cyber incidents are phishing mails, malware infections (ransomware), data exfiltration, and Distributed Denial of Service (DDoS). It is said that ransomware can cause relatively higher financial losses than phishing mails and data exfiltration are in the third place as a threat in cyberspace. Besides, someone can meet other incidents that are entitled as identity theft, steal of hardware, misuse of resources, failures of counterparties or suppliers, SQL injection, crypto jacking, and cyber risk incidents within the supply chain. More specifically insurers, in premiums they do not make crystal clear the type of malware, so in most costly threats, malware is displayed as the most frequent incident. Insurers are trying to provide complete solutions and coverage from cyber-attacks they will have to redefine their approach to a certain number of attacks. Moreover, a trend in the cyber insurance market is the fact the many customers demand from cooperating SMEs to have cyber insurance. This becomes a customer requirement, with 35% of SMEs buying these for that purpose [28].

Ransomware is a very common cyber threat. Over the last year, ransomware has gone nuclear. It is

one of the most important and widespread events used to attack cyberspace where hackers break into computers belonging to business or individuals, encrypt their data, and then demand a payment to decrypt it. Victims of such attacks find it very difficult to recover their encrypted data without paying for it. However, there are cases when they do not need to take such action as they have stored all the information on media that are not affected by the ransomware attack. The resulting cyber incidents are causing more and more problems as their frequency increases dramatically. Data breaches are security breaches in which copied, transmitted, displayed, stolen, or used sensitive, protected, or confidential data by a person who is not authorized to do so. Cyber insurance acts as a mitigation tool to respond to the rapidly growing threats in cyberspace, including ransomware. This method of attack is used because it is cheap and easy to execute, the criminals behind them usually operate in inaccessible law enforcement jurisdictions, where they are free to revise and repeat attacks as often as they wish. Currently more than half of today’s ransomware victims end up paying the ransom. Cyber-criminals have become thoughtful; taking time to maximize the targeted organization’s potential damage and their payoff. After achieving root access, the adversaries explore the network reading emails, finding data and once they know the victim, they craft a plan to cause the most panic, pain, and operational disruption. Ransomware has gone nuclear and is now responsible for tens of thousands of cybersecurity incidents and billions of dollars in paid ransom. We can observe that this is a parameter that plays an important role in the cyber insurance market. There are numerous well known cyber-attacks related to ransomware, where the victims had issues with their insurers. For instance, the well-known NotPetya attack [29] in 2017 found the victims thought to be covered for this attack. Mondelez was one the victims and the financial loss was more than $100 million. Mondelez’s insurer, Zurich Insurance, said it would not be sending a reimbursement check. It cited a common, but rarely used, clause in insurance contracts: the “war exclusion,” which protects insurers from being saddled with costs related to damage from war [30]. The same problem was identified by other well-known companies.

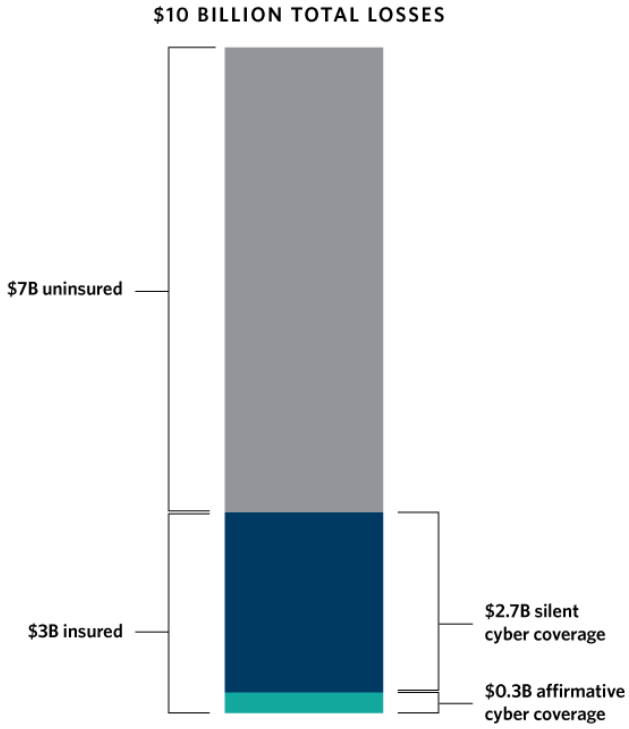

Figure 5 NotPetya's Estimated Global Losses and Insurance Impact

Most losses—about $7 billion—were not covered by any insurance policy. But the $3 billion of insured losses, and the overall magnitude of the event, surprised many in the insurance market. Industry leaders had considered the possibility of such a broad-based, high-impact cyber event, but not every insurer had fully appreciated or planned for it. NotPetya and a similar 2017 cyber-attack called WannaCry were the first modern cyber incidents to inflict such high levels of simultaneous losses on hundreds of victims in dozens of countries. This phenomenon is known in the insurance industry as "aggregation": the risk of a single peril or trigger leading to many claims at once. Aggregation risks are financially dangerous for insurers, particularly when they cut across multiple geographic regions and economic sectors. In such cases, it is difficult for insurers to limit, diversify, or swap portions of their exposure, as they might do for natural disasters [31].

Insurance companies therefore came to exclude certain war-related claims to protect their overall financial viability. In addition, there is a moral basis for war exclusions: some insurers are wary of encouraging aggression by helping to offset the costs of any blowback suffered by an aggressive state. The specific language of war exclusions varies, but they are generally written in broad terms, especially in property and casualty policies. Merck's and Mondelez's property and casualty policies are particularly broad, excluding any "hostile or warlike action in time of peace or war," whether carried out by a government or its "agent". The umbrella term "war exclusion" can therefore be misleading. It can conflate war-specific clauses with others that apply during both war and peace, and some clauses may not even require any act of violence. In the cases of Merck and Mondelez, broadly written exclusions enabled insurance companies to argue that NotPetya fit their literal terms and intent.

From the previous paragraph that depicts a real situation from a real cyber incident we can observe that ransomware is a cyber-attack that can take advantage of many different surfaces. Also, this situation raises different issues that are not only issues of misunderstanding but also issues for special coverages. Indeed, it is a unique parameter that demands attention not only from insurers but also from insureds. Its importance is understood and there are specific proposal forms covering ransomware.

Very promising is the fact that 65% of small and medium-size businesses (SMEs) are planning to spend more on cyber insurance as part of their cyber resilience plan in the next two years and 58% of large US-based enterprises plan to spend more on cyber insurance over the next two years based on a survey by Cowbell Insurance in 2020 [32]. Personal cyber insurance will become a "must-have" in personal lines insurance packages. This is a fact that has been affected from the numerous phishing attacks to individuals related to COVID-19 situation.

Moreover, the blockchain is a technology that will enter the cyber insurance market to change it. In the cyber world blockchain has the potential to impact multiple areas of the cyber insurance market. As a core infrastructure for transactions, it allows users to continuously drive greater efficiencies, reduce fraud, lower costs by decentralizing processing and ID management, and increase levels of customer satisfaction with faster validation and claims processing. Smart contracts enable blockchain users to transparently transfer anything of value without the interference of a middleman. Like physical contracts, smart contracts stipulate the rules between two parties. Unlike physical contracts, smart contracts can track insurance claims and hold both parties accountable. If any false or fraudulent claims are made by the policy owner (or if an insurance company no longer agrees to cover a condition previously agreed upon), a smart contract will immediately dissolve, and the premium payments will transfer back to the individual. The process creates a sense of mutual trust between the two parties for two reasons: all data is transparently displayed, and the slightest contractual deviation results in restitution to the harmed party. Blockchain's ability to safeguard sensitive information is especially enticing to an industry that heavily relies on data gleaned from being at the intersection of health, work, and personal life. Blockchain's ledgers are decentralized, so they cannot be corrupted or manipulated by one authority. Instead, all data is chronologically timestamped to ensure a clear recording of events. Guardtime (company that develops blockchain solutions cross the cybersecurity, government, finance, defence and logistics industries) and Maersk implement a blockchain-based maritime insurance platform that will manage risk, use smart contracts and establish an immutable chain-of-shipping to help insurance companies thoroughly provide coverage [33], [34].

5 Cyber insurance issues

In this Section, we aim to analyse the issues following the cyber insurance market which is increasing rapidly. Researchers in this deliverable aim to briefly analyse the most important issues of this market. The issues following the works in [7] and [35] are the following.

IS1. Insurers lack of experience and standards

This means that policyholders are required to have a clear understanding of their cyber risk exposures to determine the appropriate type as well as the amount of coverage required based on their specific

situation. However, 49 percent of respondents surveyed by Marsh admitted that they possess “insufficient knowledge” about their own risk exposures to assess the insurances available [36], [37]. Moreover, this includes issues related unclear coverages and exclusion that is closely related to the cyber insurance policy writing practises used by the insurers. Also, it includes issues that arise from the forensics. Also, we can observe from the investigated proposal forms that different insurers use different terminology or classifications to describe the types of the same incidents covered in cyber insurance policies., which is confusing for a prospective insured.

IS2. Evolution of system

Information technology systems rapidly evolve not only due to the dynamicity of the system itself but also because the technology involves and becomes more complex and demanding. These reasons lead to changes that are not limited to procedures but also to technological devices and innovative application. From smart devices through smart cities the emerging technologies have become an integral part of their vital procedures. It is expected that the global information security market will reach $170.4 billion in 2022 [38]. While cloud, Artificial Intelligence - also known as AI-, automation, and smart buildings (from houses until factories) undertake the leading role in working procedures, new threats emerge that jeopardise the functionality (Confidentiality, Integrity, Availability) of each information system. Nevertheless, teleworking is an upcoming trend that plays an important role in the dynamicity of an information technology system. It is verified that the teleworking skyrocketed during the year of 2020, since 40% of those currently working in the EU began to telework fulltime because of the pandemic [39]. This is an example of how easily a technological system can change and from a static one can rapidly evolve into an ad-hoc one. This change bears many issues and emerges new threats [40]. This dynamicity influences the computation of the probability of an incident and increases the difficulty of assessment and re-assessment of systems.

IS3. Information asymmetry

Information Asymmetry has a negative effect on the cyber insurance ecosystem and includes two components: i) the inability of the insurer to distinguish between insureds of different (high and low risk) types, and ii) insurers undertaking actions (i.e., reckless behaviour) that affect loss probability after the insurance contract is signed knowing that they would be insured. Reasons that lead to information asymmetry are the following: i) insurers lacking vital information regarding applications, software products installed by insureds, and security maintenance habits, which correlate to the risk types of insureds, and ii) insureds hide information about their reckless behavioural intentions from their insurers, after they get insured, knowing that they would be compensated irrespective of their malicious behaviour (e.g., being careless with security settings, etc.,) [41].

IS4. Hard to specify rate of occurrences

Most of the cyber security risk assessment methodologies contain the parameter of the rate of occurrence or probability of occurrence of an event. It is a parameter that probability that a given threat is capable of exploiting a given vulnerability. Once a list of threats has been finalized, then it is necessary to determine how possible each threat is to occur. During the risk analysis process, an overall probability that indicates the probability that a potential threat may be executed against a

specific asset will be determined. The probability parameter consists of an estimation of the likelihood that a specific threat event will be initiated with an estimation of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts). For adversarial threats, an assessment of likelihood of occurrence is typically based on: i) adversary intent; ii) adversary capability; and iii) adversary targeting. For other than adversarial threat events, the likelihood of occurrence is estimated using historical evidence, empirical data, or other factors. The likelihood of threat occurrence can also be based on the state of the organization (including for example, its core mission/business processes, enterprise architecture, information security architecture, information systems, and environments in which those systems operate)—taking into consideration predisposing conditions and the presence and effectiveness of deployed security controls to protect against unauthorized/undesirable behaviour, detect and limit damage, and/or maintain or restore mission/business capabilities [42], [43]. The difficulty for calculating these values emerges from the fact that the lack of experience and lack of historical data make this action difficult. It is difficult to determine the probability based on historical records due to lack of historical data.

IS5. Interdependence of security

There are two types of interdependence that are important in the cyber insurance field. The first one is the internal interdependence, while the second one is the external interdependence. The internal interdependence means that the assets that belong to an information system are coherent. For instance, the integration of industry 4.0 creates new instances among a smart organization (smart factory) including but not limited to automation, Internet of Things (also known as IoT), big data and cloud computing. These subsystems are interconnected and seamlessly work to achieve the highest efficiency of the organization. However, this interdependence emerges new threats. On the other hand, external interdependence plays an important role in cyber risk increasing not only its importance but also its complexity since the interconnection with systems that are out of the control of the main one bear many different risks that are inherited to it. For instance, software dependency is an example for external dependencies. There are cyber insurance proposal forms that cover losses due to external dependencies (see Section 3).

IS6. Lack of statistical data

One of the most important issues and issues that follows the cyber insurance market is the lack of statistical data regarding previous cyber-attacks. This is a fact that occurs because organizations and companies which the victims of cyber-attacks do not reveal information regarding the incident. There are numerous incidents that go unreported and undetected and there are not available for all of them details regarding the cyber-attack [12]. This issue creates difficulties for insurers to build predictive models that can assist in calculating more accurate probability of loss. Hard data is in short supply for a variety of reasons. One is that insurers have not been selling cyber insurance long enough or on a big enough scale to generate their own critical mass of data. Moreover, there is not any analytic, centralized source of information about cyber events for insurers to tap into. At the same time, the big amount regarding the reported cyber-attacks includes breaches that expose personally identifiable information (e.g., the breach occurred in Marriott Hotels [44] revealed personal data from five million guests), often because of legal notification requirements in various states. Also, denial of service

attacks and ransomware are often securely protected and are not published.

IS7. Hard to estimate damage

As we have already mentioned in the previous deliverable D3.1 [9], assets can be categorized to information and digital assets. Figure 6 presents the distinction of the assets. The difficulty for estimating the damage is cyber security risks arises from the fact that a large part of its impact is intangible. Such unpredictable impact impedes the precise pricing of the premium.

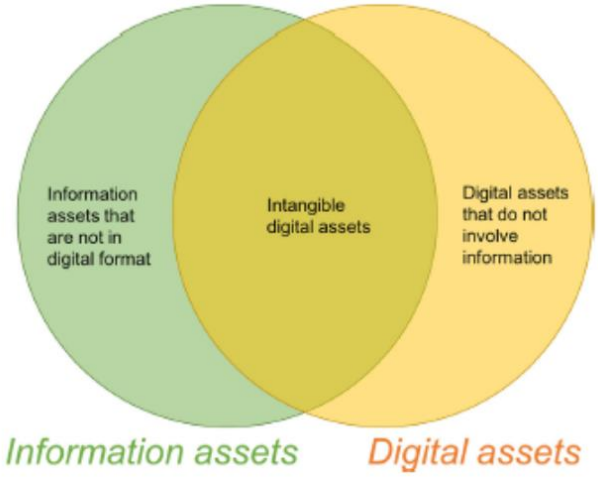

Figure 6 Categorisation of information asset and digital asset adapted from [45]

IS8. Hard to verify

This issue is related to risk management. Once the organization understands each risk that could harm the organization, then must develop a corresponding treatment plan. Understanding the importance of cyber risk management, then the organization must understand the cyber insurance framework.

IS9. Correlated risks

Security incidents correlate not only because of weak security of others, but also because of the nature of IT risks in general as well. Many information technology systems follow the same philosophy by-design and have many commonalities. This is a reason that many systems are affected by cyber hurricanes. While the more unique an information system is the less possible to be affected by a cyber hurricane outbreak. Another issue rises regarding the difficulty that the cyber insurance market meets when it must ensure systems that have information technology systems different.

IS10. Liability

This is an issue that arises due to the applications used by the insureds. Providers may be liable for not providing enough control over its customers and bear some responsibility for their malicious actions. Investigating numerous cyber insurance proposal forms, we can observe that there is a trend that

starts considering the application and services provided by third parties. The same issues arise also for the end users of each insured.

IS11. Time for claims

It is very common that many cyber-attacks remain unnoticed and the impact to the attacked organization may happen long after the first compromise. Based on [46] the average time to identify a breach in 2020 was 207 days. An example of that situation is again the breach in Marriott Hotels that initiated from 2014; the Starwood network had been compromised during the year of 2014 (during this year the Starwood was not part of the Marriott). Marriott purchased Starwood in 2016, but nearly two years later, the former Starwood hotels had not been migrated to Marriott's own reservation system and were still using IT infrastructure inherited from Starwood. Whether and when such threats should be covered is mostly the problem for correct policy writing. Also, cyber insurance proposal forms have a period (in months) so that insureds can claim even after the end of their contract.

These are the major challenges of covering cyber and are well-known in the insurance world. Insurers, insureds, and governments have worked steadily and incrementally to address them. As a result, more cyber insurance coverage is sold each year—including policies specifically created for cyber risk, as well as some traditional lines, like property and casualty insurance, that are revised to include cyber alongside other risks (adding a "cyber endorsement" to a broader policy). This growth in premiums collected has been accompanied by institutional maturation, as insurers develop more cyber expertise and refine their cyber practices. The overall sense has been one of optimism.

6 Contributions of the SECONDO platform

As we can observe from the discussion in the Sections 2-5, there are four vital fields that require attention: i) data acquisition; ii) data analysis; iii) intelligence and iv) continuous risk monitoring. The future and the efficiency of the cyber insurance market depends on covering the existing gap in these fields. The SECONDO project focuses on these four different fields (see Figure 1) and aims to fill the existing gap. In this Section, we aim to analyse how the SECONDO project through its modules and submodules aims to face the difficulties and issues that exist and emerge in this market. The SECONDO project consists of four main modules which consist of the pillar of the platform: i) Quantitative Risk analysis Module; iii) Cyber Security Investment Module; iii) Cyber Insurance and Premiums Module and iv) Continuous Risk Monitoring Module.

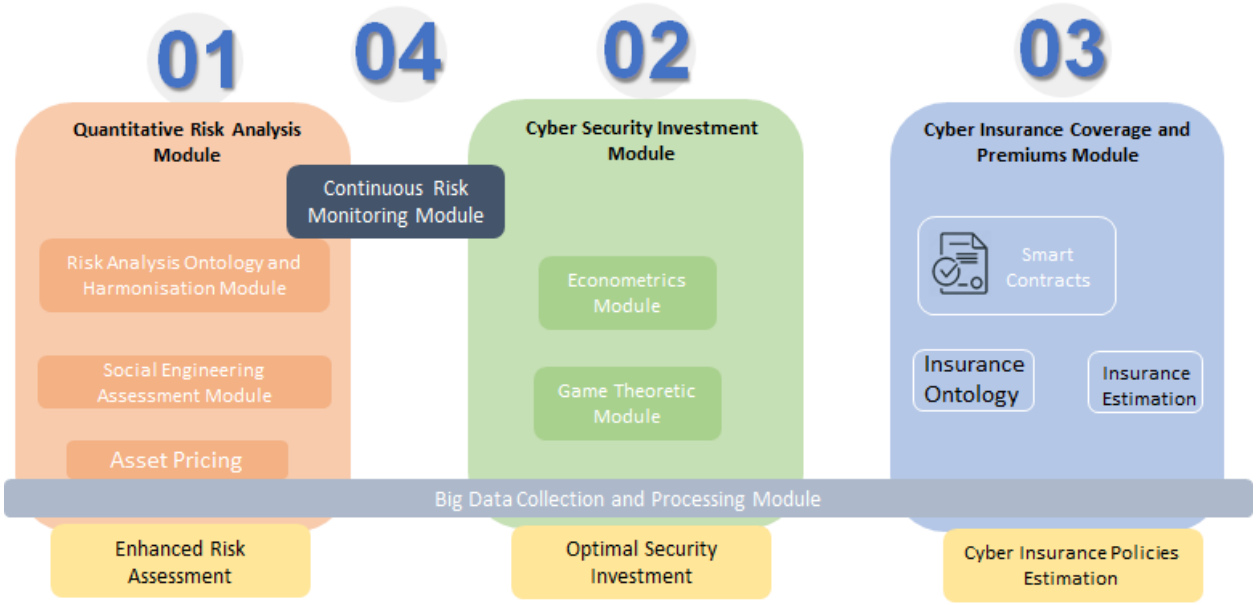

Figure 7 SECONDO reference platform architecture

- **Quantitative Risk Analysis Module**, also known as QRAM, utilises advanced security metrics to quantitatively estimate the exposed cyber risks, considering important parameters not currently considered by existing risk analysis tools [9]. SECONDO utilises advanced methodologies for digital asset identification and valuation. Qualitative and quantitative methods derived both from Business Impact Analysis and insurance pricing models are investigated to calculate the relative and intrinsic value of an organisation's digital assets. To implement the desired functionalities the following SECONDO modules have already been implemented: i) the *Risk Analysis Ontology and Harmonisation Module (RAOHM)* [4] that receives the outcomes of the existing risk analysis tools and harmonises them using a common vocabulary with straightforward definition in order to be used by QRAM; ii) the *Social Engineering Assessment Module* (*SEAM*) [9] that interacts with users to assess their behaviour using penetration testing approaches and it provides specific numeric results on risky actions, (i.e. percentage of users that open suspect files or execute Trojans, etc.); and iii) the intelligent *Big Data Collection and Processing Module (BDCPM)* that uses specialised crawlers to acquire risk-related data either from internal organisation sources, e.g. network infrastructure or external sources such as social media (this will be delivered in D3.2). These individual modules assist the entire SECONDO platform to successfully face the following issues (see Section 6): i) Insurers lack experience and standards, thought SEAM, which assess the employees' behaviour and aims to create a human firewall [36]; ii) Evolution of system, with all modules of QRAM can quantitatively estimate the cyber risk without topology limitation; iii) Hard to specify rate of occurrences, through the RAOHM that contains asset pricing methods for valuing the assets and v) Hard to estimate damage, through the RAOHM, SECONDO project can estimate the cyber risk integrating different parameters (such as user's behaviour).

- **Cyber Security Investment Module**, also known as CSIM, will be empowered by a game-theoretic approach, which is used to model defending-attacking scenarios and derive optimal defence strategies in presence of attackers that aim to cause maximum damage. Costs for attacking and defending will be investigated and they will be given as an input to CSIM. The latter will take as inputs: i) the outcome of the provided extended and QRAM, and ii) the results of BDCPM that provides analytics on Internet sources regarding state-of-the-art security solutions as well as their cost. These inputs are enhanced with the output of three complementary modules: *i) the Game Theoretic Module (GTM)* that models all possible attacking scenarios and defensive strategies, (i.e. available security controls), by employing attack graphs (this will be delivered in the upcoming deliverable D4.3); *ii) the Econometrics Module (ECM)* that provides estimates of all kinds of costs of potential attacks and it takes into account costs, (i.e. purchase, installation, execution, etc.), of each possible security control using a set of existing econometric models (this will be delivered in the upcoming deliverable D4.1); and iii) the *Continuous Risk Monitoring Module (CRMM).* All these inputs are modelled and processed by CSIM providing recommendations for optimal investments in cyber security. To take into account cyber insurance, CSIM will provide decision support for organisations that seek an optimal equilibrium point (i.e., balance) between spending on cyber security investment and cyber insurance fees. These individual modules assist the entire SECONDO platform to successfully face the following issues (see Section 6): i) Insurers lack of experience and standards, since through the GTM the organization can obtain knowledge regarding the possible attack scenarios and defensive scenarios; ii) Evolution of system, both GTM and ECM can be executed to different system without limitations providing organization the chance to test security level of the a future network topology before its implementation having time to create better cyber risk plan; iii) Hard to estimate damage, through the ECM an organization can estimate the damage from cyber-attacks, but also the cost for achieving efficient security level and iv) Correlated risks, since the GTM equips the organization with the chance to make trials for its topology or known topology and make it able to adapt it its needs but being different from classic topologies increasing the difficulty to be compromised.
- **Cyber Insurance and Premiums Module,** also known as CIPM, aims to compute premium curves and coverages as a function of the organisation's security level. These can be used by clients to determine desirable levels of cyber security investment prior to any cyber insurance contract agreement. CICPM will follow a standardised logic, which enables underwriters to incorporate their own strategy, as required by a competitive market; and, on the other hand, minimises the information asymmetry between insurer and insured. To achieve its goals, the proposed insurance calculation tool will take input from: a) the proposed QRAM; b) the defending policies selected to be applied to provide optimal protection strategies as well as the results of the related econometric parameters that justify the cost effectiveness of the considered security investments; c) analytics on cyber insurance environment and market; and d) the underwriter's strategy. In order to provide a standardized and verifiable insurance calculation model, an innovative *Cyber Insurance Ontology* will be designed and developed (this will be delivered in the upcoming deliverable D5.2). Privacy-preserving smart contracts will be leveraged to hide sensitive client information. Also, it will provide the organisation and

clients flexible smart contract description (this will be delivered in the upcoming deliverable D5.3), so that more expressive contract contents are reflected in the digital format. Last, CICPM will communicate with CRMM for monitoring the conditions that violate cyber insurance smart contract agreements toward resolving conflicts. These individual modules assist the entire SECONDO platform to successfully face the following issues (see Section 6): i) Information asymmetry, through the Cyber Insurance Ontology prospective insureds will be able to understand in-depth a proposal form without misunderstanding, since the exclusions and coverages will be clearly presented; ii) Liability, since in the ecosystem of SECONDO each organization will be insured and monitored for possible cyber incidents and iii) Time for claims, through the smart contracts which will be fed from the CRMM the insured organization (policyholder) will be monitored for possible violation of the contract, also, the claims will be automatically handled without disputes among the participants.

- **Continuous Risk Monitoring Module**, also known as CRMM, assesses on a continuous basis the performance of the implemented risk-reducing cyber security controls allowing the adaptation of the cyber insurance contract to the changing IT environment and the evolving cyber threat landscape (this will be delivered in the upcoming deliverable D4.1). This module assists the entire SECONDO platform to successfully face the following issues (see Section 6): i) Insurers lack of experience and standards, through the continuous monitoring can assist organizations to obtain experience regarding their behaviour during the contract; ii) Interdependence of security, the organization can deduce results that can reveal which asset can affect the security status of other assets in case of compromise iii) Lack of statistical data, since the CRMM store the results (cyber-attack results, occurrence, type on incident, etc.) into the private blockchain for transparency, security and evidence for the future iv) Hard to verify, through the CRMM can monitor the real time of the organization health status something can enable the organization to establish and revise its existing risk management plan.

Table 3 summarizes the aforementioned information regarding the issues that are covered from each SECONDO module. The comparison is based on the following signs: ✔, –.

- The ✔ sign declares that the respective module can effectively cover the gap of a specific issue from Section 5.
- The - sign presents that the respective module cannot cover the gap of a specific issue from Section 5.

Table 3 How SECONDO aims to cover the issues

Issue	*QRAM*	*CSIM*	*CIPM*	*CRMM*

	RAOHM	***SEAM***	***BDCPM***	***GTM***	***ECM***	***Cyber Insurance Ontology***	***Privacy-preserving smart contracts***	
IS1. Insurers lack of experience and standards	-	✓	-	✓	-	-	-	✓
IS2. Evolution of system	✓	✓	✓	✓	✓	-	-	-
IS3. Information asymmetry	-	-	-	-	-	✓	-	-
IS4. Hard to specify rate of occurrences	-	✓	✓	-	-	-	-	-
IS5. Interdependence of security	-	-	-	-	-	-	-	✓
IS6. Lack of statistical data	-	-	-	-	-	-	-	✓
IS7. Hard to estimate damage	✓	-	-	✓	✓	-	-	-
IS8. Hard to verify	-	-	-	-	-	-	-	✓
IS9. Correlated risks	-	-	-	✓	-	-	-	-
IS10. Liability	-	-	-	-	-	-	✓	-
IS11. Time for claims	-	-	-	-		✓	✓	-

Table 3 reveals that the final version of the SECONDO platform will be able to provide solutions for all the aforementioned issues (see Section 6). We can observe that each issue can be faced from at least one SECONDO submodule. One of the innovative parts of the project is the utilization of SEAM that

can enhance the experience of insureds measuring not only technical aspects but also behavioural aspects. Also, the Cyber Insurance Ontology aims to mitigate the existing gap between the insured and insurer through its output that will assist the insured to understand and identify the coverages and exclusions. Also, the historical data will be collected especially through the cooperation of BDCPM and CRMM. The BDCPM will collect the data while the CRMM will analyse them and store them with the blockchain. Finally, the CRMM will monitor in real-time any violation of the premium that will lead to specific actions (smart contracts). Besides, the health status will be monitored by CRMM providing information regarding any necessary claim. Finally, the claims handling will be faster and more efficient since smart contracts have an important role in the SECONDO ecosystem. We can observe that the SECONDO platform will abide by the existing standardization following well known standards as well as guidelines for successfully fulfilling the steps of the cyber insurance process (see Section 2).

7 Conclusion

From the above Sections, we can observe that the cyber insurance market is growing. Only a small fraction of cyber losses is currently insured. Part of the reason is that demand for cyber coverage remains limited. Many companies do not appreciate the full extent of cyber risk, or they assume that traditional insurance lines will protect them. Others recognize the risk but see cyber insurance coverage as too narrow or ambiguous to guarantee adequate recovery.

To summarize, this deliverable D5.1 “Cyber Insurance Market, Attributes and Sources” is the first of the WP5 and aims to present the status of the cyber insurance market. First and foremost, we presented the participants of this market and the stages that comprise the cyber insurance process. Furthermore, we investigated numerous cyber insurance proposal forms and we presented the most common coverages and how different insurance companies understand the business interruption following their forms. Moreover, we have presented the current trends of the market. In addition, we analysed the issues that appear as obstacles in this market and do not let it mature and finally, we analysed how the SECONDO platform manages these issues paving the way for a better, smarter, more efficient, and trustworthy cyber insurance ecosystem.

References

[1] Analysis and Valuation of Insurance Companies, Center for Excellence in Accounting and Security Analysis.

[2] Insurers’ role in EU cyber resilience, insurance europe.

[3] “THE ROLE OF INSURANCE INTERMEDIARIES,” https://www.ciab.com/wp-content/uploads/2017/04/RoleOfInsInt.pdf [Available online: last access: 15/03/2021].

[4] Neighborhood Institutions as Resource Brokers: Childcare Centers, Interorganizational Ties, and Resource Access among the Poor, MARIO LUIS SMALL,Princeton University.

[5] THE ROLE OF INSURANCE INTERMEDIARIES, WFii.

[6] Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies, 2018, Euroepan Insurance and Occupational Pensions Authority (EIOPA).

[7] Marotta, A., Martinelli, F., Nanni, S., Orlando, A. and Yautsiukhin, A., 2017. Cyber-insurance survey. Computer Science Review, 24, pp.35-61..

[8] NIST, Specification for Asset Identification1.1.

[9] SECONDO Deliverable D3.1.

[10] Common Vulnerabilities and Exposures (CVE), https://cve.mitre.org/ [Available online: last access: 15/03/2021].

[11] MITRE ATT&CK Framework, https://attack.mitre.org/ [Available online: last access: 15/03/2021].

[12] THE SECURITY RISKASSESSMENT HANDBOOKA Complete Guide for Performing Security Risk AssessmentsDOUGLAS J. LANDOL.

[13] Woods, D., Agrafiotis, I., Nurse, J.R. et al. Mapping the coverage of security controls in cyber insurance proposal forms. J Internet Serv Appl 8, 8 (2017)..

[14] Cyber Risk aware, Creating a human firewall, Whitepaper.

[15] Encouraging Clarity in Cyber Insurance Coverage, THE ROLE OF PUBLIC POLICY AND REGULATION, OECD.

[16] Baer, Walter S., and Andrew Parkinson. "Cyberinsurance in it security management." IEEE Security & Privacy 5.3 (2007): 50-56..

[17] The Council of Insurance Agents & Brokers. (2018). Summer 2018 cyber market watch survey highlights., The Council of Insurance Agents & Brokers. (2018). Summer 2018 cyber market watch survey highlights..

[18] PWC. Are insurers adequately balancing risk & opportunity? Findings from PwC’s global cyber insurance survey. 2018.

[19] ASSESSMENT OF THE CYBER INSURANCE MARKET, CISA CYBER+INFRASTRUCTURE, DECEMBER 21, 2018.

[20] Shetty, S., McShane, M., Zhang, L., Kesan, J. P, Kamhoua, C. A, Kwiat, K., & Njilla, L. L. (2018). Reducing informational disadvantages to improve cyber risk management. The Geneva Papers on Risk and Insurance-Issues and Practice, 43(2), 224–238..

[21] Stanley, C. 2017. Cyber market estimate (interview 26 June, Christian Stanley, Casualty Executive, Class of Business Underwriting Performance, Lloyd’s.

[22] PwC. 2015. Insurance 2020 & beyond: Reaping the dividends of cyber resilience.

[23] The global cyber insurance market size in the post-COVID-19 scenario is projected to grow from USD 7.8 billion in 2020 to USD 20.4 billion by 2025, at a CAGR of 21.2%, https://www.globenewswire.com/news-release/2020/10/21/2112099/0/en/The-global-cyber-insurance-market-size-in-the-post-COVID-19-scenario-is-projected-to-grow-from-USD-7-8-billion-in-2020-to-USD-20-4-billion-by-2025-at-a-CAGR-of-21-2.html [Available online: last access: 15/03/2021].

[24] Cyber Insurance Market Size, Share & Trends Analysis Report By Organization (SMB, Large Enterprise), By Application (BFS, Healthcare, IT & Telecom), And Segment Forecasts, 2019 - 2025, https://www.grandviewresearch.com/industry-analysis/cyber-insurance-market [Available online: last access: 15/03/2021].

[25] Facebook Starts Planning for Permanent Remote Workers,, Online: [Last access: 25/02/2021], https://www.nytimes.com/2020/05/21/technology/facebook-remote-work-coronavirus.html, .

[26] MMC CYBER HANDBOOK2021 Cyber Resilience Perspectives: Clarity In the Midst of Crisis.

[27] FBI sees cybercrime reports increase fourfold during COVID-19 outbreak, https://www.engadget.com/fbi-cybercrime-complaints-increase-fourfold-covid-19-091946793.html?guccounter=1 [Available online: last access: 15/03/2021]..

[28] Survey Results: The EconomicImpact of Cyber Insurance, Cowbell Insurance, 2020.

[29] The Untold Story of NotPetya, the Most Devastating Cyberattack in History, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Available online: last access: 15/03/2021]..

[30] Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong., https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html [Available online: last access: 15/03/2021].

[31] War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions, https://carnegieendowment.org/2020/10/05/war-terrorism-and-catastrophe-in-cyber-insurance-understanding-and-reforming-exclusions-pub-82819 [Available online: last access: 15/03/2021].

[32] Survey Results: The EconomicImpact of Cyber Insurance, Cowbell Insurance, 2020.

[33] Blockchain and Insurance: A Match Made In... The Near Future, https://www.zeguro.com/blog/blockchain-in-the-insurance-business [Available online: last access: 15/03/2021].

[34] Nine companies using blockchain to revolutionize insurance, https://builtin.com/blockchain/blockchain-insurance-companies [Available online: last access: 15/03/2021].

[35] Dambra, S., Bilge, L. and Balzarotti, D., 2020, May. SoK: Cyber insurance–technical challenges and a system security roadmap. In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 1367-1383). IEEE.

[36] CYBER RISK IN ASIA-PACIFICTHE CASE FOR GREATER TRANSPARENCY, Marsh, Asia pacific Risk Center.

[37] N. Kshetri, "The Economics of Cyber-Insurance," in IT Professional, vol. 20, no. 6, pp. 9-14, 1 Nov.-Dec. 2018, doi: 10.1109/MITP.2018.2874210..

[38] Forecast Analysis: Information Security, Worldwide, 2Q18 Update.

[39] Telework in the EU before and after the COVID-19: where we were, where we head to. European Commission’s science and knowledge service.

[40] Evangelakos, G., 2020. Keeping critical assets safe when teleworking is the new norm. Network security, 2020(6), pp.11-14..

[41] Pal, R., 2012. Cyber-insurance in internet security: A dig into the information asymmetry problem. arXiv preprint arXiv:1202.0884..

[42] NIST, SP 800-30 Rev. 1, Guide for Conducting Risk Assessments.

[43] Information Security Risk Analysis, Second Edition, Thomas R. Reltier.

[44] Marriott Hotels fined £18.4m for data breach that hit millions, https://www.bbc.com/news/technology-54748843 [Available online: last access: 15/03/2021].

[45] Keyun Ruan.Digital Asset Valuation and Cyber Risk Measurement: Principlesof Cybernomics. Academic Press, 2019.

[46] Cost of a Data BreachReport, 2020, IBM Security.

[47] The Council of Insurance Agents & Brokers. (2018) Summer 2018 cyber market watch survey highlights., https://www.ciab.com/resources/summer-2018-cyber-market-watch-survey-highlights/, [Available online: last access: 15/03/2021].

[48] Shetty, S., McShane, M., Zhang, L., Kesan, J. P, Kamhoua, C. A, Kwiat, K., & Njilla, L. L. (2018). Reducing informational disadvantages to improve cyber risk management. The Geneva Papers on Risk and Insurance-Issues and Practice, 43(2), 224–238..