University of Piraeus

School of Information and Communication Technologies

Department of Digital Systems

Postgraduate Program of Studies

MSc Digital Systems Security

Master Thesis

Hull Cyber Cover using the SECONDO Platform

Supervisor Professor: Dr. Xenakis Christos

Mentor: Farao Aristeidis

Name-Surname	E-mail	Student ID.
Ioannis Chouchoulis	giannischouch@ssl-unipi.gr	MTE2132

Piraeus

12/07/2023

Abstract

Nowadays, cyber risks and crimes are becoming way too common to any kind of business that invest and take advantage of the cutting-edge technologies related to the use of Internet, in order to grow bigger. Of course, there has been a great evolvement of the cyber defending services and mechanisms, but this is not enough. Various sectors of businesses, such as the maritime, which is our use case, have been facing physical attacks (e.g., piracy), but during the past few years and the technological growth of their equipment, they are endangered due to cyber-related threats and vulnerabilities. SECONDO, a European funding research project, aims to highlight a necessary and innovative approach of risk management and assessment, developing a platform of useful tools, that paves the way of a better understanding of Cyber Insurance and its concepts.

Περίληψη

Στις μέρες μας, οι κίνδυνοι και τα εγκλήματα στον κυβερνοχώρο γίνονται πολύ συνηθισμένα για κάθε είδους επιχείρηση που επενδύει και εκμεταλλεύεται τις τεχνολογίες αιχμής που σχετίζονται με τη χρήση του Διαδικτύου, προκειμένου να αναπτυχθεί περισσότερο. Φυσικά, έχει σημειωθεί μεγάλη εξέλιξη των υπηρεσιών και των μηχανισμών προστασίας στον κυβερνοχώρο, αλλά αυτό δεν αρκεί. Διάφοροι τομείς επιχειρήσεων, όπως ο ναυτιλιακός, που είναι η δική μας περίπτωση χρήσης, αντιμετώπιζαν φυσικές επιθέσεις (π.χ. πειρατεία), αλλά τα τελευταία χρόνια και με την τεχνολογική ανάπτυξη του εξοπλισμού τους, κινδυνεύουν λόγω απειλών και τρωτών σημείων που σχετίζονται με τον κυβερνοχώρο. Το SECONDO, ένα ερευνητικό έργο ευρωπαϊκής χρηματοδότησης, στοχεύει στην ανάδειξη μιας αναγκαίας και καινοτόμου προσέγγισης της διαχείρισης και αξιολόγησης κινδύνων, αναπτύσσοντας ένα πλαίσιο χρήσιμων εργαλείων, που ανοίγει το δρόμο για την καλύτερη κατανόηση της ασφάλισης στον κυβερνοχώρο και των εννοιών της.

Acknowledgements

First of all, I would like to express my gratitude to my primary supervisor, professor Christos Xenakis for his mentorship during my research. Furthermore, I would like to thank Aristeidis Farao (PhD candidate) for the guidance and feedback he provided in order to complete this thesis, as well as the rest of my colleagues at the Systems Security Lab (SSL) of University of Piraeus Research Center (UPRC). Lastly, I would be remiss in not mentioning my family and friends for their patience and support through my tight schedule.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

BC	**B**roker **C**ompany
BDCPM	**B**ig **D**ata **C**ollection and **P**rocessing **M**odule
BIMCO	**B**altic and **I**nternational **M**aritime **Co**uncil
CICPM	**C**yber **I**nsurance **C**overage and **P**remiums **M**odule
CSIM	**C**yber **S**ecurity **I**nvestment **M**odule
DDoS	**D**istributed **D**enial **o**f **S**ervice
ENISA	**E**uropean Union **A**gency for **N**etwork and **I**nformation **S**ecurity
EU	**E**uropean **U**nion
GTM	**G**ame **T**heory **M**odule
IC	**I**nsurer **C**ompany
ICT	**I**nformation and **C**ommunications **T**echnology
IMO	**I**nternational **M**aritime **O**rganization
ISPS	**I**nternational **S**hip and **P**ort Facility **S**ecurity (Code)
ISM	**I**nternational **S**afety **M**anagement (Code)
ISO	**I**nternational **O**rganization for **S**tandardization
OT	**O**perational **T**echnology
QRAM	**Q**uantitative **R**isk **A**nalysis **M**etamodel
R&D	**R**esearch & **D**evelopment
RAOHM	**R**isk **A**nalysis **O**ntology and **H**armonisation **M**odule
SC	**S**hipping **C**ompany
SEAM	**S**ocial **E**ngineering **A**ssessment **M**odule
SECONDO	a **S**ecurity **ECON**omics service platform for smart security investments and cyber insurance pricing in the beyond 2020 netw**O**rking era
SSL	**S**ystems **S**ecurity **L**ab
UPRC	**U**niversity of **P**iraeus **R**esearch **C**enter

1. Introduction

1.1 Introduction

Since 2004, a cybersecurity related agency was established, called ENISA (European Union Agency for Network and Information Security). The Union's objectives are to achieve a high common level of cybersecurity across the Europe, contribute to EU cyber policy enhance the trustworthiness of ICT (Information and Communications Technology) products, services, and processes with cybersecurity certification schemes, cooperate with Member States and EU bodies, and help Europe prepare for the cyber challenges of tomorrow [1]. One of the many interesting concepts that appeared through discussion, needs and strategies is the Cyber Insurance.

Cyber Insurance is an emerging field of cybersecurity, which can play a crucial role to the mitigation of cyber risks that are lurking to leverage the vulnerabilities that can be found at any type of business. The main concept of Cyber Insurance is almost the same as the typical insurance procedure, that people are using in other aspects of their life, such as health, car, and travel insurance. Insurance is a legal agreement between two parties – the insurer and the insured, also known as insurance coverage or insurance policy. The insurer provides financial coverage for the losses of the insured that s/he may bear under certain circumstances [2]. Of course, there can be a third party in-between the insurer and the insured, which is the insurance broker, who are professionals that serve as intermediaries and represent the insured ones.

Aiming to showcase the importance of the Cyber Insurance and its imperative use in various sectors of business, SECONDO's platform will be used upon the use case of the maritime sector, which has been technologically evolved and gave birth to cyber-related needs. An example of a shipping company is described, defining the high-level architecture, the actors and the different type of data that manages. The SECONDO platform and its sub-components receive the input (shipping company data) and provides a premium as a result.

1.2 SECONDO Project

During the last few years, the European Commission has developed several strategies in order to enhance the quality of services provided in various Internet-related aspects of European citizens' lives in the near future. One of its main priorities is the growth of the vast field of cybersecurity towards a safer Europe, focusing on R&D (Research & Development) activities.

On the same pathways, SECONDO (a Security ECONomics service platform for smart security investments and cyber insurance pricing in the beyonD 2020 netwOrking era) Project (Grant agreement ID: 823997) [3][4] is under the auspices of the HORIZON 2020, which was an EU's research and innovation funding program, that occurred from 2014 to 2020 [5]. It was initiated in January 2019 and will reach its end at the end of 2023, funded under EXCELLENT SCIENCE - Marie Skłodowska-Curie Actions.

Figure 1 - SECONDO Logo

SECONDO's main objective is to assist businesses and professionals who are looking for comprehensive, well-researched security strategies and investments in cyber security that support human decision-making. Given the expected continued growth of cyberattacks, this research problem is one that needs to be addressed now. Normal business operations and the EU society itself are seriously threatened by this growth. Setting a budget, selecting an investment strategy for cyber security, and purchasing cyber insurance in the face of uncertainty are extremely difficult tasks with significant business repercussions. SECONDO wants to have an impact on how EU businesses operate because they frequently: (i) have a small budget for cyber security; and (ii) downplay the value of cyber insurance. Cyber risk can be significantly reduced with the help of cyber insurance. This can be achieved by making companies pay a premium for their exposure to cyber risk, with the possibility of paying a lower premium should they lower their current exposure.

In order to support cutting-edge software, the SECONDO Project combines engineering and mathematical insights, providing a platform that bridges the gap between the theoretical knowledge and practice. For that reason, the consortium of these project includes both industrial and academic partners, aiming for a better understanding of the business needs and the development of the platform.

In the context of SECONDO Project, some scenarios and Use Cases have been created in order to test the under-development components, using the right requirements and business data that occur in real life, towards the completion of the platform.

In this thesis, the Use Case of maritime, which will be furthermore elaborated in its dedicated section below, is selected to showcase the efficiency of some of the components, that have been already developed and tested, and will be described in detail in the next chapter, highlighting the importance of Cyber Insurance in the end.

2. SECONDO Components

This section and its sub-sections are focused on providing information and specific descriptions of each sub-component of the SECONDO Platform, that will be used in this thesis.

SECONDO Platform includes several components that have been developed in parallel, but each component could work as a standalone. In the context of the project, there is logic path, that composes the main architecture of the platform, where for each Use Case, the components results are input to next-in-line components, aiming to the final calculation of the premium, which is the ultimate goal of the platform and the project itself.

In this thesis, specific components from the whole SECONDO Platform have been selected to be demonstrated, which are enough to showcase the results of the Use Case of maritime. These components are SEAM, GTM, RAOHM, Crawlers and CICPM, and whose functionality is described briefly below.

Social Engineering Assessment Module

Social Engineering Assessment Module (SEAM) aims to identify all the types of vulnerabilities of the assets, collected from the business data, and is part of a higher-level component, QRAM (Quantitative Risk Analysis Metamodel), that employs advanced security metrics to provide a quantitative assessment of cyber risks, considering key parameters that are often overlooked by existing risk analysis tools. These parameters include social engineering and pre-existing information. The QRAM component comprises two subcomponents, namely the SEAM and the Risk Analysis Ontology and Harmonization (RAOHM). Furthermore, SEAM is a tool whose main purpose is to interact with the users and extract insightful information with regards their cyber-awareness [6]. More specifically, the tool calculation and evaluation answer the question whether the employees of any organization are ready to stand against social engineering attacks. Social engineering refers to all techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons [7]. Such techniques could be phishing emails or impersonating an important client aiming to browse malicious websites. Thus, SEAM's purpose is to receive input from the organization and extract useful insights related to social engineering data, that will be used by the next component, the RAOHM.

Risk Analysis Ontology and Harmonisation Module

Risk Analysis Ontology and Harmonisation Module is also part of a higher-level component, QRAM, as SEAM. RAOHM is a special tool, which combines all concepts that are related to the SECONDO Project, including risks and threats. [6]. In addition, RAOHM provides a mechanism that combines the knowledge of the emerging threat landscape and the countermeasures based on the current literature, aiming to decrease the probability of security incidents to the assets of an organization and developing an aggregated risk analysis ontology, where the vulnerabilities, threats, defensive strategies, and risk management analysis insights can be shared among stakeholders of the same or different organizations. In particular, RAOHM's purpose is to receive input from SEAM (Social Engineering Data) and the existing Risk Analysis tools, such as CORAS [8], and provide an insightful Harmonized Metamodel as output.

Big Data Collection and Processing Module - Crawlers

Big Data Collection and Processing Module (BDCPM) is the component that leverages specific crawlers in order to gather risk-related data the come from several sources. The sources could be the organizations themselves, such as network infrastructure insights, but also the Internet, such as social media (Twitter) or other external sources. The main purpose of this tool is to construct an aggregated database, acquiring various types of data, regardless their source, since the BDCPM is interconnected with the rest of the components. In this context, the stored data could be processed and used in such ways in order to build predictive models, that would clarify emerging cyberattacks. The conducted analytics and results would be beneficial for the organizations, aiming for developing the right defensive strategies [6]. Thus, BDCPM makes use of specialized crawlers, collects reports and data from other components, such as CSIM and CICPM, and aims to provide cyber security domain analytics, that are being processed in order to achieve improved estimations during the calculations of the premiums.

Game Theory Module

Game Theory Module (GTM) is a sub-component of CSIM (Cyber Security Investment Module), which provides recommendations for optimal investments in cyber security. GTM’s main service is to create all the possible attacking scenarios and defensive strategies, using the attack graphs, based on the Bayesian game-theoretic approach. [6]. In more technical detail, high-level attack scenarios, that may endanger the assets and data of any organization, are modeled, and then several defensive strategies and solutions will be produced, depending on the method (proactive or reactive depending on the way and time of the applied defensive strategies). Thus, GTM’s purpose is to receive risk assessment data and analytics as input and provide optimal defending strategies and solutions to the organization [9][10].

Cyber Insurance Coverage and Premiums Module

Cyber Insurance Coverage and Premiums Module (CICPM) is one of the basic components, that was developed in the scope of SECONDO Platform. This tool actually calculates the premium and coverages of an organization from the security level aspect. In this way, the stakeholders would be able to make the optimal decision of investing to a cyber insurance contract. Since the component of CICPM is the last-in-line module in SECONDO's architecture, its purpose is to gather all the data collected and used by previous components (CSIM) like reports that include cyber insurance violations of the contract agreement. In addition, it receives as inputs insights with regards to risk assessment, strategies, and analytics and then, it extracts an insurance exposure assessment and the estimated cyber insurance premiums and coverage as the final result, without violating privacy-preserving information [6][11].

All the above-mentioned components, their interconnections, and the inputs/ outputs of each one of them are presented in a high-level architecture overview in the figure below.

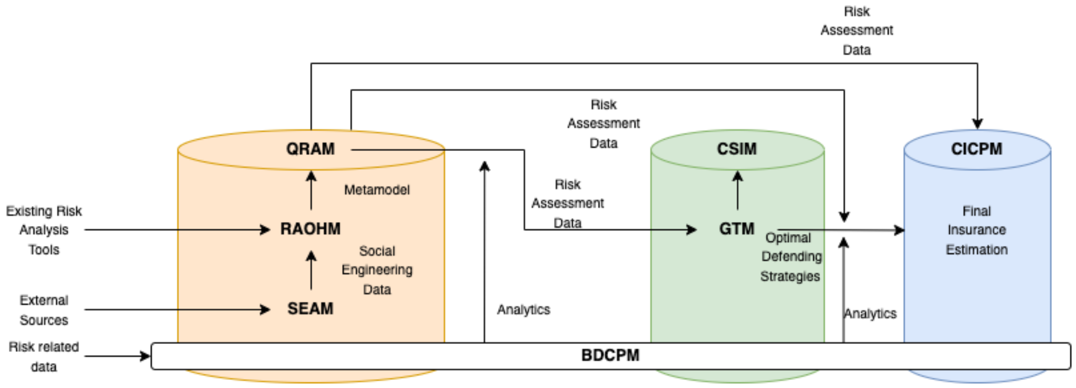


Figure 2 - High-level Architecture Overview

3. Maritime Use Case and Assets Architecture

Cyber insurance is becoming increasingly important in the maritime industry due to the growing threat of cyber-attacks. The maritime industry relies heavily on technology and digital systems to operate efficiently, making it vulnerable to cyber threats such as hacking, data breaches, ransomware, and malware attacks. These types of incidents can result in significant financial losses, loss of sensitive data, and damage to a company's reputation. For that reason, cyber insurance can provide protection against these risks by covering the costs of responding to and recovering from a cyber-attack, as well as providing access to resources and expertise to help minimize the impact of the attack. Additionally, it can help organizations meet regulatory requirements, as well as demonstrate to customers, shareholders, and partners that they take the threat of cyber-attacks seriously and have taken appropriate steps to protect their sensitive information and systems. With the rapid pace of technological change and the growing sophistication of cyber attackers, having a robust cyber insurance policy in place is becoming essential for any organization operating in the maritime industry.

In the following sections of this chapter, the use case of maritime is described in detail, showcasing an attack scenario and the data included.

3.1 Motivation and Real-life Examples

The vast sector of maritime is a crucial aspect of the trade and transportation industry and has seen various forms of threats over the years, with physical attacks such as piracy being a common issue. However, with the advancement of technology and the widespread adoption of electronic systems in onshore and onboard environments, cyber and cyber-physical vulnerabilities have emerged as a new concern.

There are several examples of cybersecurity-related incidents that have been occurred in the vast field of maritime during the last few years. One of the most famous incidents is the Maersk cyber-attack in 2017, which was a large-scale ransomware attack that affected the Danish shipping and logistics company A.P. Moller-Maersk. The attack occurred on June 27, 2017, and was caused by the NotPetya malware, which spread rapidly throughout the company's network and affected its operations globally. The attack caused significant disruptions to Maersk's operations, including the shutdown of its IT systems, the disabling of critical applications, and the disruption of communications. The company had to halt operations at several container terminals, including the one in the Port of Rotterdam, and was forced to use manual processes to manage cargo at many of its other terminals. According to reports, the Maersk cyber-attack caused the company losses of up to $300 million. The attack was also significant in its impact on the wider shipping industry, as other companies that relied on Maersk's systems were also affected. The attack highlighted the vulnerability of the shipping industry to cyber-attacks and the need for companies to improve their cybersecurity measures. Maersk later reported that it had implemented significant improvements to its cybersecurity, including the establishment of a new cybersecurity risk management system [12].

There are also other examples like this one back in 2018, when the shipping company Cosco, that suffered a cyber-attack that impacted its IT systems, resulting in widespread disruptions to its operations and the loss of sensitive commercial information [13]. Also in 2018, the port of San Diego was hit by a cyber-attack that impacted its computer systems, causing delays to its operations [14]. More recently, in 2021, the Norwegian ship management company Vard was hit by a ransomware and forced its shut down [15].

In the same pathways, an interesting report from LLOYD’s was published in October 2019, which depicts the economic disaster of a hypothetical scenario. This report examines the potential impact of a cyber-attack on major ports throughout Asia Pacific, with the worst-case scenario estimating losses of up to $110 billion. The hypothetical "Shen Attack" presents a plausible situation in which a computer virus is transported by ships, infecting 15 ports, and causing chaos by scrambling cargo database records. The report demonstrates that an attack of this scale would have significant economic consequences for a wide range of global business sectors due to the interconnectedness of the maritime supply chain. The transportation, aviation, and aerospace sectors would be the most affected, with a total of $28.2 billion in economic losses, followed by manufacturing ($23.6 billion) and retail ($18.5 billion). Indirect economic losses would also impact every country that has bilateral trade with the affected ports, with Asia expected to bear the brunt of the damage, losing up to $27 billion. The report highlights the lack of preparation and insurance coverage for such a catastrophic event, with only 8% of the total economic costs insured, leaving a massive insurance gap of $101 billion [16].

In this context, one issue that has arisen in the wake of these cyber threats is the lack of coverage provided by insurance policies. Typically, indirect damages caused by cyber-attacks or errors would not be covered under non-cyber insurance policies due to the inclusion of a cyber-attack exclusion clause, which states that insurers will not cover damages caused by a cyber-attack if they include bodily harm, business interruption, or property damage. This is referred to as the "cyber insurance gap" (Cl. 380) [17]. However, due to the increase in incidents of cyber-attacks, there has been growing discussion about expanding coverage for such events. It is becoming clear that the impact of a cyber-attack is not limited to just digital assets and can have far-reaching consequences for companies.

Due to the growing field of the cyber insurance, and there are many aspects of its procedures and policies that are yet to be determined, such as the distinction between affirmative and silent or non-affirmative cyber insurance. Affirmative cyber insurance clearly states in the insurance policy that the insurer will cover the costs in the event of a data breach, network failure, or attack, regardless of the impact, while silent or non-affirmative cyber insurance refers to unquantified exposures that result from cyber-attacks or incidents and may affect traditional property.

However, there is still much unknown about cyber risks and new challenges arise as technologies evolve. One of these is that unfortunately few incidents of cyber-attacks in the marine sector are being reported or made public, leading to a false sense of security among marine companies. As a result, this underreporting misguides many companies to purchase basic insurance policies, either disregarding cyber risks or assuming they are included in the coverage, leading to miscommunication and misunderstandings between companies and insurers. Insurers face difficulties in managing coverage capacity, risk estimation, and appropriate solutions, leading to the existence of unintended or silent cyber coverage. If a cyber-attack causes damage to a company's physical equipment, network failure, or business interruption, it is possible that an insurer may not have the capacity for coverage. In some cases, insurance companies may charge a premium for non-affirmative cyber coverage but given the rapidly evolving technologies and increasing number of cyber incidents, this may not be a sustainable solution.

To mitigate the risk of financial loss from a cyber-attack, shipping companies can transfer their risk to third party organizations, named insurance companies. This is done by purchasing an insurance policy, which provides coverage against financial risks. The risk transfer process involves risk assessment, risk management, and insurance exposure estimation, coverage, and premium calculation. However, it is important to note that standard hull and machinery insurance does not cover various costs associated with a cyber-attack, such as breach response costs, income loss, third-party costs, and regulatory fines [18].

3.2 Description of Use Case and Scenario

In this thesis, the use case of the Hull Cyber Cover is highlighted, which is based on a shipping company named "Captain's Shipping Inc" and located in Athens, Greece, aiming to insure its ship. Its annual revenue is estimated around 500.000 € and the necessary information, that are crucial for the insurance procedure, but also for the premium calculation using the SECONDO Platform are being presented in detail in the following Chapter 4.1.5, providing a clear picture during the execution of the use case.

Furthermore, the basic asset categories of the shipping company of the scenario are:

i. Human actors (e.g., crew, operators),

ii. Data (various types of them such as customer (personal/business/financial) data, route, cargo, vessel, logistics, personnel data). These are categorized as Critical Files within the SECONDO ecosystem,

iii. Communication systems (e.g., LAN, satellite),

iv. Sensors (e.g., thrust meter, wind anemometer),

v. Navigation System (e.g., GPS),

vi. Cargo Management System,

vii. Propulsion System and

viii. Mooring System.

Physical and cyber-attacks could endanger the proper operation of such assets, causing severe problems not only to the financial state of the shipping company, but also to its reputation, and unfortunately sometimes to its employees' lives.

Furthermore, there are 3 main parties that take part in this use case:

I. The shipping company ("Captain's Shipping Inc."), a business entity that operates ships, vessels or any other marine transportation means to move cargo and people from one place to another. Shipping companies are typically exposed to a wide range of cyber risks, including ransomware attacks, data breaches, and system failures, among others. In the context of cyber insurance, shipping companies seek coverage for potential losses resulting from cyber incidents, as well as risk management services to mitigate their exposure to cyber threats,

II. The broker ("Broker and Broker Inc."), which is a licensed intermediary who helps clients (shipping companies) navigate the insurance market and find the most suitable coverage for their cyber risks. Brokers act as intermediaries between the insured party and the insurer, and they typically have access to multiple insurance carriers to help clients find the best possible coverage and premiums. Brokers may assist clients in assessing their cyber risks and identifying the specific types of coverage they need, such as data breach response, business interruption, and network security liability. They can also provide guidance on risk management strategies and offer ongoing support to clients throughout the policy period. Brokers may charge a fee or commission for their services, which is typically paid by the insurer, and

III. The insurer ("Shipsurer Inc."), which is the company that provides the insurance policy to the insured party (shipping company). The insurer assumes the risk of potential losses related to cyber incidents in exchange for a premium paid by the policyholder. The insurer also provides the policyholder with coverage for losses related to cyber incidents as specified in the insurance policy. In the event of a claim, the insurer is responsible for investigating the claim, determining the validity of the claim, and paying out the appropriate amount to the policyholder based on the terms of the policy.

In this context, there are 3 main stages of the insurance process, which is interconnected with the SECONDO components:

1. Risk Assessment: This is the first step, which is completed after using specific external tools. The results that come of such tools, are being used as input to the RAOHM component. RAOHM processes that information and forwards it towards QRAM. At the same time, SEAM will evaluate the harm posed by adversaries who aim to target the ship, systems, equipment, and personnel of the shipping firm through cyber-attacks, as well as the reactions and actions of the shipping company's staff in regard to cybersecurity. Then, the shipping company will provide their proposed insurance coverage based on their assets and assessed risks.

2. Risk Management: The second step includes the GTM, which calculates all potential attack scenarios, the best courses of action for defense, and the cost estimates for each security control using existing econometric models. The outputs are forwarded towards CSIM and used to generate optimal investment recommendations.

3. Cyber Insurance Exposure estimation, Coverage and Premium calculation: For the third and final step, CICPM gathers the outputs of the previously mentioned modules to determine the computed insurance premium and coverage. Since the premium is set by the insurer, the broker communicates with the shipping company to review the contract and explain the premium. If the shipping company agrees to the premium and coverage, the three parties (shipping company, broker, and insurer) reach a final agreement. During the whole process, CICPM stays in communication with the CSIM to monitor for any potential violations of the contract.

Our scenario in this thesis states that our shipping company “Captain’s Shipping Inc” (SC), through the broker company of “Broker & Broker Inc” (BC), has already “signed” a smart contract with the insurer company “Shipsurer” (IC). In order for the SC to be relieved by the general risk, the IC consults the SC, which requests coverage for its claims. Of course, the IC requests from the SC the necessary information and data related to the compliance aspects with various guidelines.

There are several compliance guidelines and bodies, that shipping companies in the maritime industry must adhere to, including:

- BIMCO (Baltic and International Maritime Council) Cyber Security Guidelines: Developed by the Baltic and International Maritime Council, these guidelines provide a platform for managing cyber risks in the shipping industry.

- International Maritime Organization (IMO): The IMO is a specialized agency of the United Nations that sets standards for the safety, security, and environmental performance of international shipping.

- International Ship and Port Facility Security Code (ISPS Code): Developed by the IMO, the ISPS Code outlines security measures that shipping companies and port facilities must take to prevent security incidents.

- International Safety Management (ISM) Code: Also developed by the IMO, the ISM Code sets standards for the safe operation of ships and pollution prevention.

- ISO Cybersecurity Standards: The International Organization for Standardization (ISO) has developed several standards related to cybersecurity, including ISO/IEC 27001, which outlines best practices for information security management systems.

At this point, with the use of RAOHM, IC should perform a secondary risk assessment in order to calculate the potential damage, premium and coverage.

In general, any SC’s asset that is cyber-related, such as local networks, databases, mails etc., could cause critical damages to the company’s operations, finances and of course reputation. On top of that, it should not be underestimated that these operational technology (OT) related risks (e.g., SCADA) may affect physical property, such as cargo and machinery, the environment and the most important, people’s safety. With a clearer view of the risks and costs involved, the IC uses GTM to calculate the most efficient ways of action and incident response strategies. Once these steps have been completed, the SC and IC come to an agreement on the strategies, premium and coverage required by SC, all of which are set out in the smart contract. The main prerequisites of SC in order to reach an agreement are (i) the obligation to follow and apply all the advice and guidelines by the IC (technical or not), (ii) the mutual understanding and full cooperation with the IC’s team during all the processes (e.g., investigations in incidents), and (iii) the continuous maintenance of its defensive cyber-related systems against threats and attacks.

In general, cyber insurance policies can vary widely in their coverage. There are several examples of costs, that are common to every occasion such as:

- Data Breach Response expenses: This can include a range of costs that a company may incur in response to a data breach. For example, it may include costs associated with hiring a forensic investigation team to determine the scope of the breach, notifying affected individuals, offering credit monitoring services, and providing legal counsel [19].
- Cyber Extortion: This can include costs associated with responding to a ransomware attack, where a hacker may demand payment in exchange for returning access to the company's systems or data. This may include the cost of hiring a professional negotiator, or even the cost of paying the ransom itself [20].
- Business interruption losses: A cyber-attack can disrupt a company's normal business operations, resulting in lost income. For example, if a company's website is taken down by a distributed denial-of-service (DDoS) attack, it may be unable to process orders or generate revenue during the downtime. Cyber insurance policies may cover the income that is lost as a result of such an attack [21].
- Damage to computer systems or data: A cyber-attack can cause damage to a company's computer systems or data, which may require significant resources to repair or replace. Cyber insurance policies may cover the cost of restoring or replacing damaged hardware or software, as well as recovering lost or corrupted data.
- Liability claims: A cyber-attack can result in legal claims against a company, such as a class action lawsuit by individuals affected by a data breach. Cyber

insurance policies may cover the cost of defending against such claims, as well as any damages that may be awarded [22].

It's worth noting that these are just a few examples of the costs that may be covered under a cyber insurance policy, and the specific terms and conditions of coverage can vary widely between policies. It's important to carefully review the terms of any policy you are considering to fully understand what is covered and what is excluded, such as Income Loss during time retention (Table 1).

Hull Cyber Cover may contain the following coverages by the IC:

Table 1: Hull Cyber Coverages Examples

Expenses	**Covered by IC (Yes / No)**
Data Breach Response	Yes
Cyber Extortion / Ransomware Payments	Yes
Business Interruption Losses / Income Loss	Yes
Physical Damages (cyber-related attack)	Yes
Data Damages (cyber-related attack)	Yes
Liability	Yes
Regulatory / Compliance Penalties	Yes
Restoration	Yes
Income Loss during time retention	No

In this context, an attack scenario is elaborated aiming to showcase the importance of Cyber Insurance and the tools that were developed in the lifecycle of SECONDO Project.

3.3 Attack Scenario

The attack scenario begins in the middle of the Atlantic Ocean, where the crew of the cargo ship "Marine Star" operated by the shipping company SC, suddenly finds their electronic systems unresponsive. A member of the crew identifies the incident and soon the headquarters of SC realize that the ship has fallen victim to a sophisticated ransomware attack known as "SeaLock" carried out by the cybercriminal group "Black Wave".

The ransomware is designed specifically to target OT systems used by the shipping industry, including SC's ship navigation, communication, and cargo management systems. The ransomware encrypts all critical files and systems, including the navigation and communication systems, making it impossible for the crew to steer the ship, communicate with the mainland or other vessels, or receive essential weather updates. The ship's engine control systems are also compromised, leading to significant disruptions in the propulsion and navigation of the vessel. As a result, the ship becomes stranded in the middle of the ocean, posing a severe risk to the crew's safety and the environment.

The attack is initially launched through a phishing email that contains a malicious link. Once an employee of SC clicks the link, the ransomware is able to gain access to the company's systems and begin to spread throughout the network.

The cybercriminals behind the attack demand a ransom of 1,000 bitcoin, equivalent to millions of dollars, to be paid within 72 hours. The ransomware is designed to escalate the consequences of non-payment, increasing the amount demanded, and leaking sensitive information to the public. The criminals are also known for their willingness to engage in other illegal activities, such as selling the stolen data on the dark web.

SC's management team immediately notifies their IT department and the IC, who advise them to engage with the cybersecurity experts and negotiate with the attackers. The cybersecurity experts assess the situation and identify the ransomware's origin, characteristics, and severity. They also estimate the time and cost required to restore the systems and data and negotiate with the attackers to reduce the ransom amount and extend the payment deadline. There also assembled some teams with specific action points related to the emergency response to such incidents and the recovery of the business continuity.

At the same time the IC is in continuous contact with the SC, cooperating to ensure that all the required actions have taken place and the incident is being treated properly. Paying the ransom amount is the last option, since the efforts are focused on restoring the damages on the ship's equipment, back up the sensitive data and business operations data. In order for these actions to be effective, there should have been a recent back up and installed tools that would be useful against such attack. Of course, the main actions are towards the safety of the crew of the ship, but also communicate with the other interested parties (clients) that are informed of the incident, ensuring the SC's reputation.

In case of some of these critical issues are not addressed, the IC would advise the SC to pay the ransom. Thus, since the incident is active, the investigation on behalf of IC is initiated, in order to receive all possible feedback and data towards the assessment of the situation and the decision making of whether the SC has been compliant through the insurance contract with the IC.

3.4 Description of Assets Architecture

In this section, the SC's assets and their characteristics are being presented, providing a high-level architecture of the ecosystem they create. These assets will be the initial input to the SECONDO tools towards the final calculation of the premiums and coverage.

In general, there are several assets on the ship "Marine Star". There are Computers and Servers, where vital Software is installed on. There are also assigned Operators that are responsible for each Asset and Procedure, aiming to ensure the prompt operation of the ship and its crew.

In the following table, the SC's assets are presented with the interconnections and the responsible operators.

Table 2: List of Assets with information

Asset Name	Asset Type	IsUsedBy	Connected to
Computer 1	Hardware	itadmin1, itadmin2	isConnectedTo: Gateway, Server 1, Server 2
Computer 2	Hardware	itadmin2, commops1, commops2	isConnectedTo: Gateway, Server 1, Server 2
Computer 3	Hardware	itadmin2, senops1, senops2	isConnectedTo: Gateway, Server 1, Server 2
Computer 4	Hardware	itadmin2, navops1, navops2	isConnectedTo: Gateway, Server 1, Server 2
Computer 5	Hardware	itadmin2, cargoops1, cargoops2	isConnectedTo: Gateway, Server 1, Server 2
Computer 6	Hardware	itadmin2, propops1, propops2	isConnectedTo: Gateway, Server 1, Server 2
Computer 7	Hardware	itadmin2, moorops1, moorops2	isConnectedTo: Gateway, Server 1, Server 2
Overview Monitoring Tool	Software	manageradmin, itadmin1, itadmin2	isInstalledIn: Computer 1
Satelite	Software	manageradmin, itadmin2, commops1	isInstalledIn: Computer 2
Weather Prediction Tool	Software	manageradmin, itadmin2, senops1	isInstalledIn: Computer 3
Thrust Meter Tool	Software	manageradmin, itadmin2, senops2	isInstalledIn: Computer 3
Wind Anemometer Tool	Software	manageradmin, itadmin2, senops1	isInstalledIn: Computer 3
GPS Tool	Software	manageradmin, itadmin2, navops1	isInstalledIn: Computer 4
Radar Tool	Software	manageradmin, itadmin2, navops2	isInstalledIn: Computer 4
Autopilot Tool	Software	manageradmin, itadmin2, navops1	isInstalledIn: Computer 4

Asset Name	Asset Type	IsUsedBy	Connected to
Cargo Management Tool	Software	manageradmin, itadmin2, cargoops1	isInstalledIn: Computer 5
Propulsion Management Tool	Software	manageradmin, itadmin2, propops1	isInstalledIn: Computer 6
Mooring Management Tool	Software	manageradmin, itadmin2, moorops1	isInstalledIn: Computer 7
MS Outlook	Software	manageradmin, itadmin1, itadmin2	isInstalledIn: Computer 1, Computer 2, Computer 3, Computer 4, Computer 5, Computer 6, Computer 7
Server 1	Hardware	manageradmin, itadmin1, itadmin2	isConnectedTo: Gateway
Server 2	Hardware	manageradmin, itadmin1, itadmin2	isConnectedTo: Gateway
Firewall	Network	manageradmin, itadmin1	isConnectedTo: Gateway
Gateway	Network	manageradmin, itadmin1	
BackUp	Procedure	itadmin1, itadmin2	isLocatedIn: Server 2
Access Control	Procedure	itadmin1, itadmin2	isLocatedIn: Server 1
Services Data	Data	itadmin1	isLocatedIn: Server 2
Tools Data	Data	itadmin1, itadmin2	isLocatedIn: Server 2

All these assets are possible cyber-targets, since they are connected to Internet and with each other, endangering the entire ecosystem and crew.

In the following table are listed the assets and the possible cyber-attacks that may leverage the security gaps.

Table 3: Possible Cyber-Attacks

Asset Name	Asset Type	Possible Cyber-Attacks
Overview Monitoring Tool	Software	Firmware Tampering, Command Injection
Satelite	Software	Signal Jamming, Spoofing, Man-In-The-Middle
Weather Prediction Tool	Software	Command Injection, Data Manipulation
Thrust Meter Tool	Software	Command Injection, Data Manipulation
Wind Anemometer Tool	Software	Command Injection, Data Manipulation
GPS Tool	Software	Signal Jamming, Spoofing, Man-In-The-Middle
Radar Tool	Software	Signal Jamming, Spoofing, Man-In-The-Middle
Autopilot Tool	Software	Signal Jamming, Spoofing, Man-In-The-Middle
Cargo Management Tool	Software	Supply Chain Attack
Propulsion Management Tool	Software	Signal Jamming, Spoofing, Man-In-The-Middle
Mooring Management Tool	Software	Signal Jamming, Spoofing, Man-In-The-Middle
Firewall	Network	Firewall Bypass, Denial-of-Service, Firewall Rule Manipulation
Gateway	Network	Distributed Denial-of-Service, Man-In-The-Middle, Spoofing, Zero-Days Exploits
BackUp	Procedure	Data Breach/ Encryption, Ransomware
Access Control	Procedure	Brute-Force Attack, Remote Exploitation, Password Spraying, Phishing, Social Engineering
Services Data	Data	Data Breach/ Encryption, Ransomware
Tools Data	Data	Data Breach/ Encryption, Ransomware

4. Execution of Use Case and Results

In this section, the execution of the abovementioned use case with the use of the selected components of the SECONDO Platform is described, accompanied with the necessary figures, aiming to highlight the efficiency and significance of such framework in the field of Cyber Insurance and Maritime.

4.1 Use Case Demonstration with the SECONDO Components

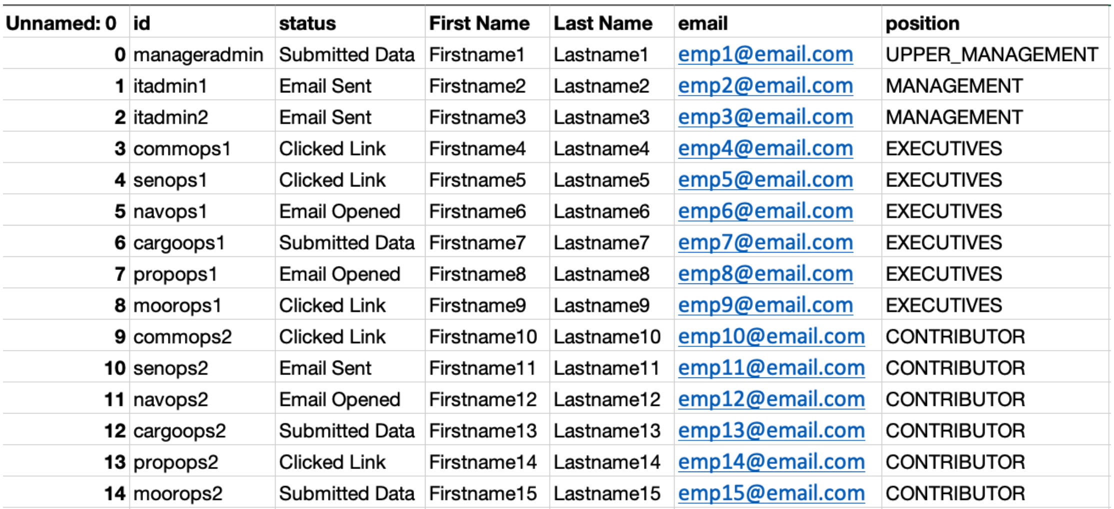
As presented in Chapter 2, the showcased components are the Social Engineering Assessment Module (SEAM), Risk Analysis Ontology and Harmosiation Module (RAOHM), Big Data Collection and Processing Module (BDCPM), Game Theory Module (GTM) and the Cyber Insurance Coverage and Premiums Module (CICPM), and the actual implementation of the use case, its involved assets and the attack scenario is described towards the final calculation of the premium.

4.1.1 SEAM

The first step is to setup the input for the Social Engineering Assessment Module, where the details of the scenario's actors are described. Since SEAM extracts insights related to their cyber-awareness, a phishing email campaign was performed, and the results are being processed by the tool.

In the Figure 3, the input has the following data:

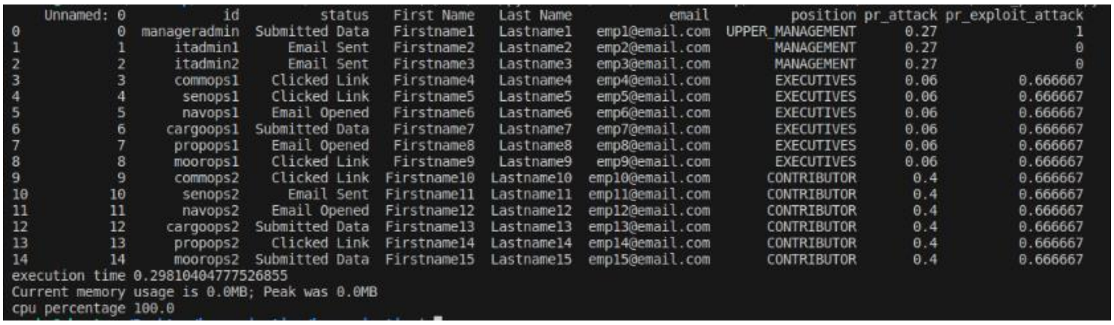
- A unique number,
- An id, which is the role and position in the ship,
- A status, which is the action that was performed during the phishing campaign by the actors,
- First / Last name and email
- Position in the hierarchy of the shipping company, based on the clearance of actions they performed.



Unnamed: 0	id	status	First Name	Last Name	email	position
0	manageradmin	Submitted Data	Firstname1	Lastname1	emp1@email.com	UPPER_MANAGEMENT
1	itadmin1	Email Sent	Firstname2	Lastname2	emp2@email.com	MANAGEMENT
2	itadmin2	Email Sent	Firstname3	Lastname3	emp3@email.com	MANAGEMENT
3	commops1	Clicked Link	Firstname4	Lastname4	emp4@email.com	EXECUTIVES
4	senops1	Clicked Link	Firstname5	Lastname5	emp5@email.com	EXECUTIVES
5	navops1	Email Opened	Firstname6	Lastname6	emp6@email.com	EXECUTIVES
6	cargoops1	Submitted Data	Firstname7	Lastname7	emp7@email.com	EXECUTIVES
7	propops1	Email Opened	Firstname8	Lastname8	emp8@email.com	EXECUTIVES
8	moorops1	Clicked Link	Firstname9	Lastname9	emp9@email.com	EXECUTIVES
9	commops2	Clicked Link	Firstname10	Lastname10	emp10@email.com	CONTRIBUTOR
10	senops2	Email Sent	Firstname11	Lastname11	emp11@email.com	CONTRIBUTOR
11	navops2	Email Opened	Firstname12	Lastname12	emp12@email.com	CONTRIBUTOR
12	cargoops2	Submitted Data	Firstname13	Lastname13	emp13@email.com	CONTRIBUTOR
13	propops2	Clicked Link	Firstname14	Lastname14	emp14@email.com	CONTRIBUTOR
14	moorops2	Submitted Data	Firstname15	Lastname15	emp15@email.com	CONTRIBUTOR

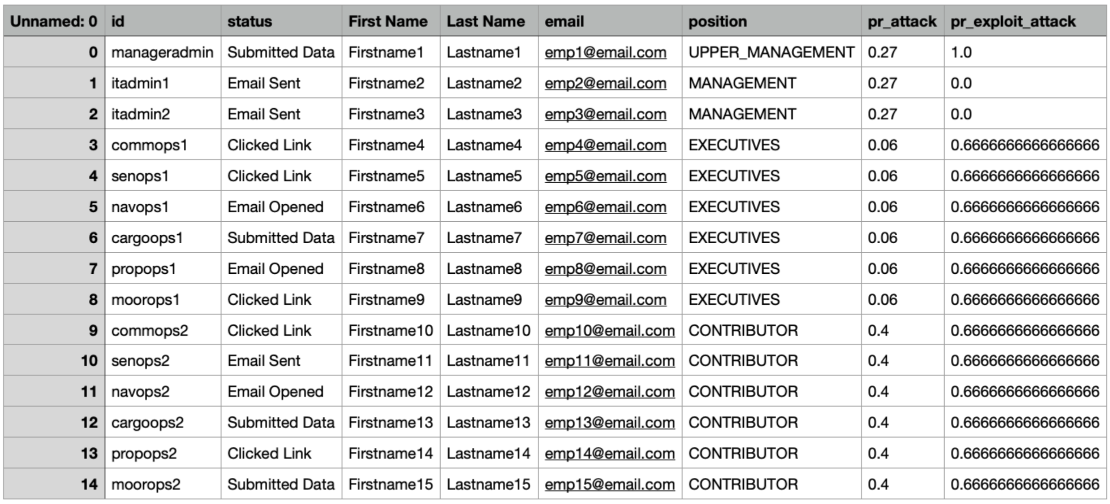
Figure 3 - Input for SEAM

In the following Figures, the execution and the outcome of the SEAM tool are presented, where the probabilities of attacking and exploiting the shipping company’s assets are calculated.



```
    Unnamed: 0           id          status  First Name   Last Name            email          position pr_attack pr_exploit_attack
0            0  manageradmin  Submitted Data  Firstname1   Lastname1   emp1@email.com  UPPER_MANAGEMENT      0.27                 1
1            1      itadmin1      Email Sent  Firstname2   Lastname2   emp2@email.com        MANAGEMENT      0.27                 0
2            2      itadmin2      Email Sent  Firstname3   Lastname3   emp3@email.com        MANAGEMENT      0.27                 0
3            3      commops1    Clicked Link  Firstname4   Lastname4   emp4@email.com        EXECUTIVES      0.06          0.666667
4            4       senops1    Clicked Link  Firstname5   Lastname5   emp5@email.com        EXECUTIVES      0.06          0.666667
5            5       navops1    Email Opened  Firstname6   Lastname6   emp6@email.com        EXECUTIVES      0.06          0.666667
6            6     cargoops1  Submitted Data  Firstname7   Lastname7   emp7@email.com        EXECUTIVES      0.06          0.666667
7            7      propops1    Email Opened  Firstname8   Lastname8   emp8@email.com        EXECUTIVES      0.06          0.666667
8            8      moorops1    Clicked Link  Firstname9   Lastname9   emp9@email.com        EXECUTIVES      0.06          0.666667
9            9      commops2    Clicked Link Firstname10  Lastname10  emp10@email.com       CONTRIBUTOR       0.4          0.666667
10          10       senops2      Email Sent Firstname11  Lastname11  emp11@email.com       CONTRIBUTOR       0.4          0.666667
11          11       navops2    Email Opened Firstname12  Lastname12  emp12@email.com       CONTRIBUTOR       0.4          0.666667
12          12     cargoops2  Submitted Data Firstname13  Lastname13  emp13@email.com       CONTRIBUTOR       0.4          0.666667
13          13      propops2    Clicked Link Firstname14  Lastname14  emp14@email.com       CONTRIBUTOR       0.4          0.666667
14          14      moorops2  Submitted Data Firstname15  Lastname15  emp15@email.com       CONTRIBUTOR       0.4          0.666667
execution time 0.29810404777526855
Current memory usage is 0.0MB; Peak was 0.0MB
cpu percentage 100.0
```

Figure 4 - Execution of SEAM



Unnamed: 0	id	status	First Name	Last Name	email	position	pr_attack	pr_exploit_attack
0	manageradmin	Submitted Data	Firstname1	Lastname1	emp1@email.com	UPPER_MANAGEMENT	0.27	1.0
1	itadmin1	Email Sent	Firstname2	Lastname2	emp2@email.com	MANAGEMENT	0.27	0.0
2	itadmin2	Email Sent	Firstname3	Lastname3	emp3@email.com	MANAGEMENT	0.27	0.0
3	commops1	Clicked Link	Firstname4	Lastname4	emp4@email.com	EXECUTIVES	0.06	0.6666666666666666
4	senops1	Clicked Link	Firstname5	Lastname5	emp5@email.com	EXECUTIVES	0.06	0.6666666666666666
5	navops1	Email Opened	Firstname6	Lastname6	emp6@email.com	EXECUTIVES	0.06	0.6666666666666666
6	cargoops1	Submitted Data	Firstname7	Lastname7	emp7@email.com	EXECUTIVES	0.06	0.6666666666666666
7	propops1	Email Opened	Firstname8	Lastname8	emp8@email.com	EXECUTIVES	0.06	0.6666666666666666
8	moorops1	Clicked Link	Firstname9	Lastname9	emp9@email.com	EXECUTIVES	0.06	0.6666666666666666
9	commops2	Clicked Link	Firstname10	Lastname10	emp10@email.com	CONTRIBUTOR	0.4	0.6666666666666666
10	senops2	Email Sent	Firstname11	Lastname11	emp11@email.com	CONTRIBUTOR	0.4	0.6666666666666666
11	navops2	Email Opened	Firstname12	Lastname12	emp12@email.com	CONTRIBUTOR	0.4	0.6666666666666666
12	cargoops2	Submitted Data	Firstname13	Lastname13	emp13@email.com	CONTRIBUTOR	0.4	0.6666666666666666
13	propops2	Clicked Link	Firstname14	Lastname14	emp14@email.com	CONTRIBUTOR	0.4	0.6666666666666666
14	moorops2	Submitted Data	Firstname15	Lastname15	emp15@email.com	CONTRIBUTOR	0.4	0.6666666666666666

Figure 5 - Outcome of SEAM

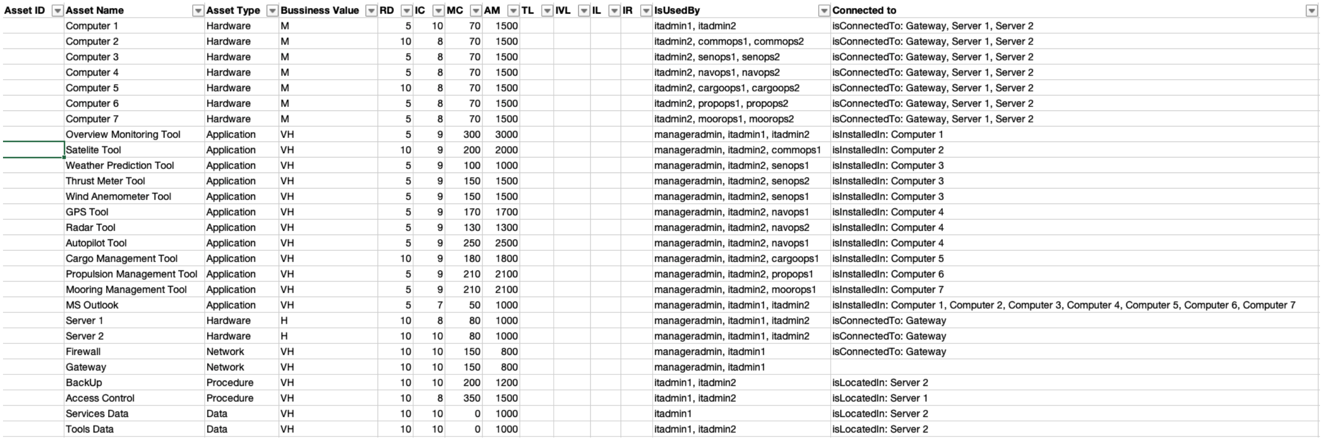
The outcome of the SEAM tool will be part of the input of the RAOHM.

4.1.2 RAOHM

The next step is to setup the input for the Risk Analysis Ontology and Harmonisation Module, where the details of the scenario's assets are described. RAOHM needs the input from SEAM and several data related to the assets in order to provide a detailed report of Harmonized Metamodel as output.

In the Figure 6, the input has the following data:

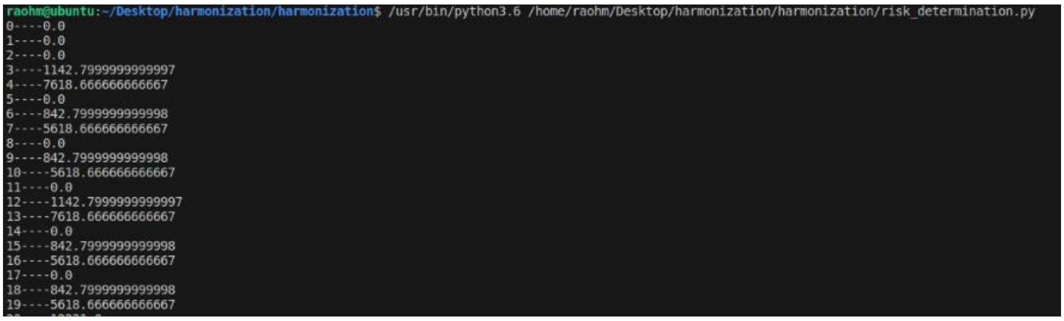
- An Asset ID, which is unique,
- An Asset Name, which describes the asset operation on the ship,
- An Asset Type, which describes the kind of asset's types (Hardware, Application, Network, Procedure, Data),
- The Business Value (Very High (VH), High (H), Medium (M), Low (L), Very Low (VL))
- Several types of cost related to the assets and the shipping company (Annual Cost, Reputation Damage, Impact Continuity, Asset Value),
- The tag "IsUsedBy", where the actors are listed,
- The tag "ConnectedTo", where the interconnections among the assets are listed.



Asset ID	Asset Name	Asset Type	Bussiness Value	RD	IC	MC	AM	TL	IVL	IL	IR	IsUsedBy	Connected to
	Computer 1	Hardware	M	5	10	70	1500					itadmin1, itadmin2	isConnectedTo: Gateway, Server 1, Server 2
	Computer 2	Hardware	M	10	8	70	1500					itadmin2, commops1, commops2	isConnectedTo: Gateway, Server 1, Server 2
	Computer 3	Hardware	M	5	8	70	1500					itadmin2, senops1, senops2	isConnectedTo: Gateway, Server 1, Server 2
	Computer 4	Hardware	M	5	8	70	1500					itadmin2, navops1, navops2	isConnectedTo: Gateway, Server 1, Server 2
	Computer 5	Hardware	M	10	8	70	1500					itadmin2, cargoops1, cargoops2	isConnectedTo: Gateway, Server 1, Server 2
	Computer 6	Hardware	M	5	8	70	1500					itadmin2, propops1, propops2	isConnectedTo: Gateway, Server 1, Server 2
	Computer 7	Hardware	M	5	8	70	1500					itadmin2, moorops1, moorops2	isConnectedTo: Gateway, Server 1, Server 2
	Overview Monitoring Tool	Application	VH	5	9	300	3000					manageradmin, itadmin1, itadmin2	isInstalledIn: Computer 1
	Satelite Tool	Application	VH	10	9	200	2000					manageradmin, itadmin2, commops1	isInstalledIn: Computer 2
	Weather Prediction Tool	Application	VH	5	9	100	1000					manageradmin, itadmin2, senops1	isInstalledIn: Computer 3
	Thrust Meter Tool	Application	VH	5	9	150	1500					manageradmin, itadmin2, senops2	isInstalledIn: Computer 3
	Wind Anemometer Tool	Application	VH	5	9	150	1500					manageradmin, itadmin2, senops1	isInstalledIn: Computer 3
	GPS Tool	Application	VH	5	9	170	1700					manageradmin, itadmin2, navops1	isInstalledIn: Computer 4
	Radar Tool	Application	VH	5	9	130	1300					manageradmin, itadmin2, navops2	isInstalledIn: Computer 4
	Autopilot Tool	Application	VH	5	9	250	2500					manageradmin, itadmin2, navops1	isInstalledIn: Computer 4
	Cargo Management Tool	Application	VH	10	9	180	1800					manageradmin, itadmin2, cargoops1	isInstalledIn: Computer 5
	Propulsion Management Tool	Application	VH	5	9	210	2100					manageradmin, itadmin2, propops1	isInstalledIn: Computer 6
	Mooring Management Tool	Application	VH	5	9	210	2100					manageradmin, itadmin2, moorops1	isInstalledIn: Computer 7
	MS Outlook	Application	VH	5	7	50	1000					manageradmin, itadmin1, itadmin2	isInstalledIn: Computer 1, Computer 2, Computer 3, Computer 4, Computer 5, Computer 6, Computer 7
	Server 1	Hardware	H	10	8	80	1000					manageradmin, itadmin1, itadmin2	isConnectedTo: Gateway
	Server 2	Hardware	H	10	10	80	1000					manageradmin, itadmin1, itadmin2	isConnectedTo: Gateway
	Firewall	Network	VH	10	10	150	800					manageradmin, itadmin1	isConnectedTo: Gateway
	Gateway	Network	VH	10	10	150	800					manageradmin, itadmin1	
	BackUp	Procedure	VH	10	10	200	1200					itadmin1, itadmin2	isLocatedIn: Server 2
	Access Control	Procedure	VH	10	8	350	1500					itadmin1, itadmin2	isLocatedIn: Server 1
	Services Data	Data	VH	10	10	0	1000					itadmin1	isLocatedIn: Server 2
	Tools Data	Data	VH	10	10	0	1000					itadmin1, itadmin2	isLocatedIn: Server 2

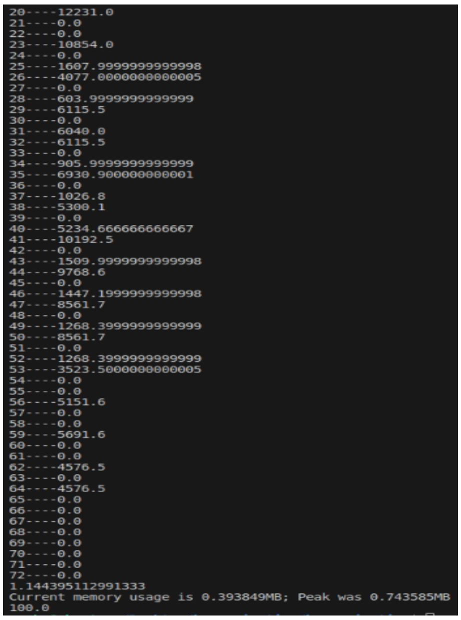
Figure 6 - Input for RAOHM

In the following Figures, the execution, and the outcome of the RAOHM tool are presented, where the risk of each asset is calculated. The outcome of the RAOHM provides a detailed report of the interconnections between the assets and the users, the estimated probability of exploiting these assets and the calculated risk for each one of them, depending on the value and the interconnections.



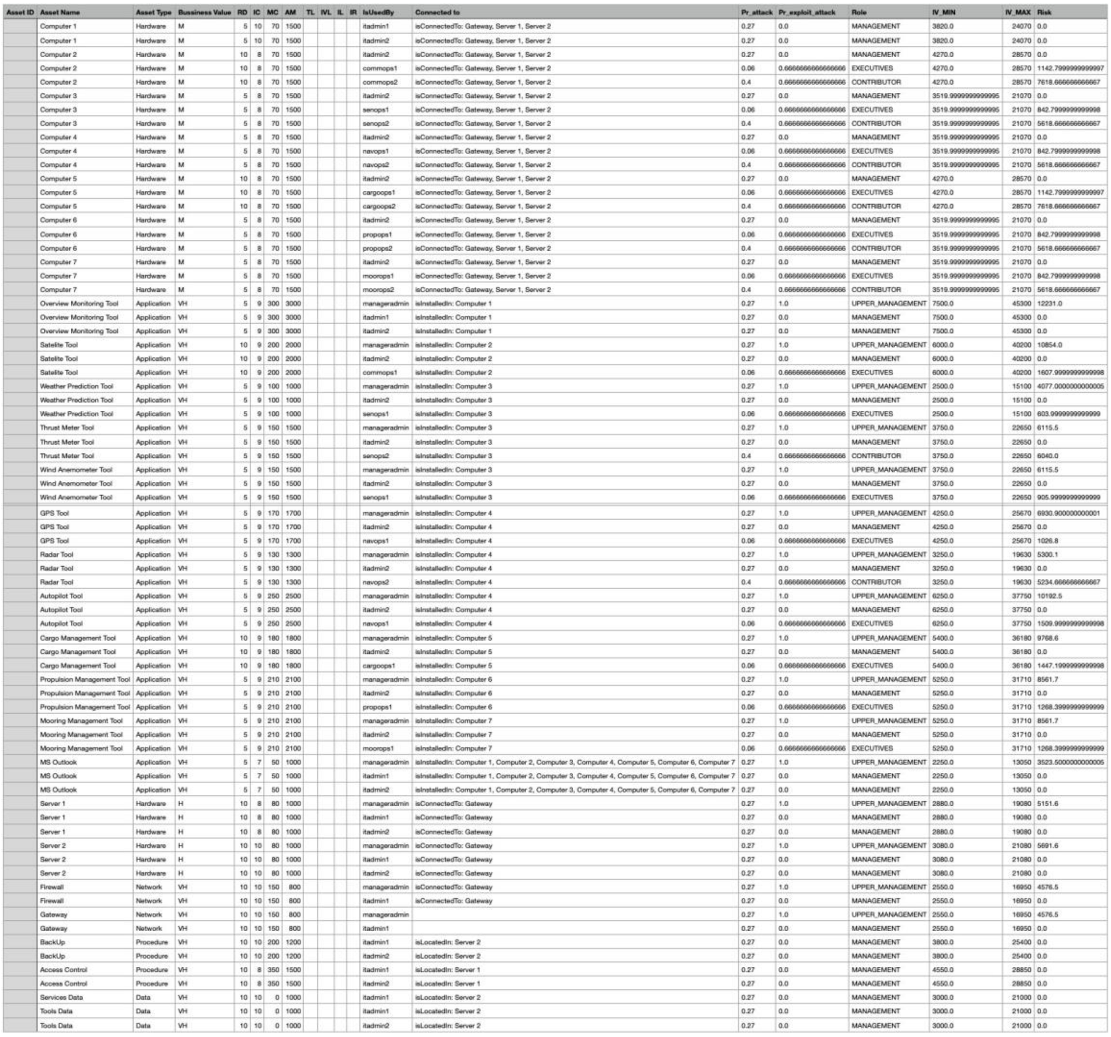
```
raohm@ubuntu:~/Desktop/harmonization/harmonization$ /usr/bin/python3.6 /home/raohm/Desktop/harmonization/harmonization/risk_determination.py
0----0.0
1----0.0
2----0.0
3----1142.7999999999997
4----7618.666666666667
5----0.0
6----842.7999999999998
7----5618.666666666667
8----0.0
9----842.7999999999998
10----5618.666666666667
11----0.0
12----1142.7999999999997
13----7618.666666666667
14----0.0
15----842.7999999999998
16----5618.666666666667
17----0.0
18----842.7999999999998
19----5618.666666666667
```

Figure 7 - Execution of RAOHM (1)



```
20----12231.0
21----0.0
22----0.0
23----10854.0
24----0.0
25----1607.9999999999998
26----4077.0000000000005
27----0.0
28----603.9999999999999
29----6115.5
30----0.0
31----6040.0
32----6115.5
33----0.0
34----905.9999999999999
35----6930.900000000001
36----0.0
37----1026.8
38----5300.1
39----0.0
40----5234.666666666667
41----10192.5
42----0.0
43----1509.9999999999998
44----9768.6
45----0.0
46----1447.1999999999998
47----8561.7
48----0.0
49----1268.3999999999999
50----8561.7
51----0.0
52----1268.3999999999999
53----3523.5000000000005
54----0.0
55----0.0
56----5151.6
57----0.0
58----0.0
59----5691.6
60----0.0
61----0.0
62----4576.5
63----0.0
64----4576.5
65----0.0
66----0.0
67----0.0
68----0.0
69----0.0
70----0.0
71----0.0
72----0.0
1.144395112991333
Current memory usage is 0.393849MB; Peak was 0.743585MB
100.0
```

Figure 8 - Execution of RAOHM (2)



Asset ID	Asset Name	Asset Type	Bussiness Value	RD	IC	MC	AM	TL	IVL	IL	IR	IsUsedBy	Connected to	Pr_attack	Pr_exploit_attack	Role	IV_MIN	IV_MAX	Risk
	Computer 1	Hardware	M	5	10	70	1500					itadmin1	isConnectedTo: Gateway, Server 1, Server 2	0.27	0.0	MANAGEMENT	3820.0	24070	0.0
	Computer 1	Hardware	M	5	10	70	1500					itadmin2	isConnectedTo: Gateway, Server 1, Server 2	0.27	0.0	MANAGEMENT	3820.0	24070	0.0
	Computer 2	Hardware	M	10	8	70	1500					itadmin2	isConnectedTo: Gateway, Server 1, Server 2	0.27	0.0	MANAGEMENT	4270.0	28570	0.0
	Computer 2	Hardware	M	10	8	70	1500					commops1	isConnectedTo: Gateway, Server 1, Server 2	0.06	0.6666666666666666	EXECUTIVES	4270.0	28570	1142.7999999999997
	Computer 2	Hardware	M	10	8	70	1500					commops2	isConnectedTo: Gateway, Server 1, Server 2	0.4	0.6666666666666666	CONTRIBUTOR	4270.0	28570	7618.666666666667
	Computer 3	Hardware	M	5	8	70	1500					itadmin2	isConnectedTo: Gateway, Server 1, Server 2	0.27	0.0	MANAGEMENT	3519.9999999999995	21070	0.0
	Computer 3	Hardware	M	5	8	70	1500					senops1	isConnectedTo: Gateway, Server 1, Server 2	0.06	0.6666666666666666	EXECUTIVES	3519.9999999999995	21070	842.7999999999998
	Computer 3	Hardware	M	5	8	70	1500					senops2	isConnectedTo: Gateway, Server 1, Server 2	0.4	0.6666666666666666	CONTRIBUTOR	3519.9999999999995	21070	5618.666666666667
	Computer 4	Hardware	M	5	8	70	1500					itadmin2	isConnectedTo: Gateway, Server 1, Server 2	0.27	0.0	MANAGEMENT	3519.9999999999995	21070	0.0
	Computer 4	Hardware	M	5	8	70	1500					navops1	isConnectedTo: Gateway, Server 1, Server 2	0.06	0.6666666666666666	EXECUTIVES	3519.9999999999995	21070	842.7999999999998
	Computer 4	Hardware	M	5	8	70	1500					navops2	isConnectedTo: Gateway, Server 1, Server 2	0.4	0.6666666666666666	CONTRIBUTOR	3519.9999999999995	21070	5618.666666666667
	Computer 5	Hardware	M	10	8	70	1500					itadmin2	isConnectedTo: Gateway, Server 1, Server 2	0.27	0.0	MANAGEMENT	4270.0	28570	0.0
	Computer 5	Hardware	M	10	8	70	1500					cargoops1	isConnectedTo: Gateway, Server 1, Server 2	0.06	0.6666666666666666	EXECUTIVES	4270.0	28570	1142.7999999999997
	Computer 5	Hardware	M	10	8	70	1500					cargoops2	isConnectedTo: Gateway, Server 1, Server 2	0.4	0.6666666666666666	CONTRIBUTOR	4270.0	28570	7618.666666666667
	Computer 6	Hardware	M	5	8	70	1500					itadmin2	isConnectedTo: Gateway, Server 1, Server 2	0.27	0.0	MANAGEMENT	3519.9999999999995	21070	0.0
	Computer 6	Hardware	M	5	8	70	1500					propops1	isConnectedTo: Gateway, Server 1, Server 2	0.06	0.6666666666666666	EXECUTIVES	3519.9999999999995	21070	842.7999999999998
	Computer 6	Hardware	M	5	8	70	1500					propops2	isConnectedTo: Gateway, Server 1, Server 2	0.4	0.6666666666666666	CONTRIBUTOR	3519.9999999999995	21070	5618.666666666667
	Computer 7	Hardware	M	5	8	70	1500					itadmin2	isConnectedTo: Gateway, Server 1, Server 2	0.27	0.0	MANAGEMENT	3519.9999999999995	21070	0.0
	Computer 7	Hardware	M	5	8	70	1500					moorops1	isConnectedTo: Gateway, Server 1, Server 2	0.06	0.6666666666666666	EXECUTIVES	3519.9999999999995	21070	842.7999999999998
	Computer 7	Hardware	M	5	8	70	1500					moorops2	isConnectedTo: Gateway, Server 1, Server 2	0.4	0.6666666666666666	CONTRIBUTOR	3519.9999999999995	21070	5618.666666666667
	Overview Monitoring Tool	Application	VH	5	9	300	3000					manageradmin	isInstalledIn: Computer 1	0.27	1.0	UPPER_MANAGEMENT	7500.0	45300	12231.0
	Overview Monitoring Tool	Application	VH	5	9	300	3000					itadmin1	isInstalledIn: Computer 1	0.27	0.0	MANAGEMENT	7500.0	45300	0.0
	Overview Monitoring Tool	Application	VH	5	9	300	3000					itadmin2	isInstalledIn: Computer 1	0.27	0.0	MANAGEMENT	7500.0	45300	0.0
	Satelite Tool	Application	VH	10	9	200	2000					manageradmin	isInstalledIn: Computer 2	0.27	1.0	UPPER_MANAGEMENT	6000.0	40200	10854.0
	Satelite Tool	Application	VH	10	9	200	2000					itadmin2	isInstalledIn: Computer 2	0.27	0.0	MANAGEMENT	6000.0	40200	0.0
	Satelite Tool	Application	VH	10	9	200	2000					commops1	isInstalledIn: Computer 2	0.06	0.6666666666666666	EXECUTIVES	6000.0	40200	1607.9999999999998
	Weather Prediction Tool	Application	VH	5	9	100	1000					manageradmin	isInstalledIn: Computer 3	0.27	1.0	UPPER_MANAGEMENT	2500.0	15100	4077.0000000000005
	Weather Prediction Tool	Application	VH	5	9	100	1000					itadmin2	isInstalledIn: Computer 3	0.27	0.0	MANAGEMENT	2500.0	15100	0.0
	Weather Prediction Tool	Application	VH	5	9	100	1000					senops1	isInstalledIn: Computer 3	0.06	0.6666666666666666	EXECUTIVES	2500.0	15100	603.9999999999999
	Thrust Meter Tool	Application	VH	5	9	150	1500					manageradmin	isInstalledIn: Computer 3	0.27	1.0	UPPER_MANAGEMENT	3750.0	22650	6115.5
	Thrust Meter Tool	Application	VH	5	9	150	1500					itadmin2	isInstalledIn: Computer 3	0.27	0.0	MANAGEMENT	3750.0	22650	0.0
	Thrust Meter Tool	Application	VH	5	9	150	1500					senops2	isInstalledIn: Computer 3	0.4	0.6666666666666666	CONTRIBUTOR	3750.0	22650	6040.0
	Wind Anemometer Tool	Application	VH	5	9	150	1500					manageradmin	isInstalledIn: Computer 3	0.27	1.0	UPPER_MANAGEMENT	3750.0	22650	6115.5
	Wind Anemometer Tool	Application	VH	5	9	150	1500					itadmin2	isInstalledIn: Computer 3	0.27	0.0	MANAGEMENT	3750.0	22650	0.0
	Wind Anemometer Tool	Application	VH	5	9	150	1500					senops1	isInstalledIn: Computer 3	0.06	0.6666666666666666	EXECUTIVES	3750.0	22650	905.9999999999999
	GPS Tool	Application	VH	5	9	170	1700					manageradmin	isInstalledIn: Computer 4	0.27	1.0	UPPER_MANAGEMENT	4250.0	25670	6930.900000000001
	GPS Tool	Application	VH	5	9	170	1700					itadmin2	isInstalledIn: Computer 4	0.27	0.0	MANAGEMENT	4250.0	25670	0.0
	GPS Tool	Application	VH	5	9	170	1700					navops1	isInstalledIn: Computer 4	0.06	0.6666666666666666	EXECUTIVES	4250.0	25670	1026.8
	Radar Tool	Application	VH	5	9	130	1300					manageradmin	isInstalledIn: Computer 4	0.27	1.0	UPPER_MANAGEMENT	3250.0	19630	5300.1
	Radar Tool	Application	VH	5	9	130	1300					itadmin2	isInstalledIn: Computer 4	0.27	0.0	MANAGEMENT	3250.0	19630	0.0
	Radar Tool	Application	VH	5	9	130	1300					navops2	isInstalledIn: Computer 4	0.4	0.6666666666666666	CONTRIBUTOR	3250.0	19630	5234.666666666667
	Autopilot Tool	Application	VH	5	9	250	2500					manageradmin	isInstalledIn: Computer 4	0.27	1.0	UPPER_MANAGEMENT	6250.0	37750	10192.5
	Autopilot Tool	Application	VH	5	9	250	2500					itadmin2	isInstalledIn: Computer 4	0.27	0.0	MANAGEMENT	6250.0	37750	0.0
	Autopilot Tool	Application	VH	5	9	250	2500					navops1	isInstalledIn: Computer 4	0.06	0.6666666666666666	EXECUTIVES	6250.0	37750	1509.9999999999998
	Cargo Management Tool	Application	VH	10	9	180	1800					manageradmin	isInstalledIn: Computer 5	0.27	1.0	UPPER_MANAGEMENT	5400.0	36180	9768.6
	Cargo Management Tool	Application	VH	10	9	180	1800					itadmin2	isInstalledIn: Computer 5	0.27	0.0	MANAGEMENT	5400.0	36180	0.0
	Cargo Management Tool	Application	VH	10	9	180	1800					cargoops1	isInstalledIn: Computer 5	0.06	0.6666666666666666	EXECUTIVES	5400.0	36180	1447.1999999999998
	Propulsion Management Tool	Application	VH	5	9	210	2100					manageradmin	isInstalledIn: Computer 6	0.27	1.0	UPPER_MANAGEMENT	5250.0	31710	8561.7
	Propulsion Management Tool	Application	VH	5	9	210	2100					itadmin2	isInstalledIn: Computer 6	0.27	0.0	MANAGEMENT	5250.0	31710	0.0
	Propulsion Management Tool	Application	VH	5	9	210	2100					propops1	isInstalledIn: Computer 6	0.06	0.6666666666666666	EXECUTIVES	5250.0	31710	1268.3999999999999
	Mooring Management Tool	Application	VH	5	9	210	2100					manageradmin	isInstalledIn: Computer 7	0.27	1.0	UPPER_MANAGEMENT	5250.0	31710	8561.7
	Mooring Management Tool	Application	VH	5	9	210	2100					itadmin2	isInstalledIn: Computer 7	0.27	0.0	MANAGEMENT	5250.0	31710	0.0
	Mooring Management Tool	Application	VH	5	9	210	2100					moorops1	isInstalledIn: Computer 7	0.06	0.6666666666666666	EXECUTIVES	5250.0	31710	1268.3999999999999
	MS Outlook	Application	VH	5	7	50	1000					manageradmin	isInstalledIn: Computer 1, Computer 2, Computer 3, Computer 4, Computer 5, Computer 6, Computer 7	0.27	1.0	UPPER_MANAGEMENT	2250.0	13050	3523.5000000000005
	MS Outlook	Application	VH	5	7	50	1000					itadmin1	isInstalledIn: Computer 1, Computer 2, Computer 3, Computer 4, Computer 5, Computer 6, Computer 7	0.27	0.0	MANAGEMENT	2250.0	13050	0.0
	MS Outlook	Application	VH	5	7	50	1000					itadmin2	isInstalledIn: Computer 1, Computer 2, Computer 3, Computer 4, Computer 5, Computer 6, Computer 7	0.27	0.0	MANAGEMENT	2250.0	13050	0.0
	Server 1	Hardware	H	10	8	80	1000					manageradmin	isConnectedTo: Gateway	0.27	1.0	UPPER_MANAGEMENT	2880.0	19080	5151.6
	Server 1	Hardware	H	10	8	80	1000					itadmin1	isConnectedTo: Gateway	0.27	0.0	MANAGEMENT	2880.0	19080	0.0
	Server 1	Hardware	H	10	8	80	1000					itadmin2	isConnectedTo: Gateway	0.27	0.0	MANAGEMENT	2880.0	19080	0.0
	Server 2	Hardware	H	10	10	80	1000					manageradmin	isConnectedTo: Gateway	0.27	1.0	UPPER_MANAGEMENT	3080.0	21080	5691.6
	Server 2	Hardware	H	10	10	80	1000					itadmin1	isConnectedTo: Gateway	0.27	0.0	MANAGEMENT	3080.0	21080	0.0
	Server 2	Hardware	H	10	10	80	1000					itadmin2	isConnectedTo: Gateway	0.27	0.0	MANAGEMENT	3080.0	21080	0.0
	Firewall	Network	VH	10	10	150	800					manageradmin	isConnectedTo: Gateway	0.27	1.0	UPPER_MANAGEMENT	2550.0	16950	4576.5
	Firewall	Network	VH	10	10	150	800					itadmin1	isConnectedTo: Gateway	0.27	0.0	MANAGEMENT	2550.0	16950	0.0
	Gateway	Network	VH	10	10	150	800					manageradmin		0.27	1.0	UPPER_MANAGEMENT	2550.0	16950	4576.5
	Gateway	Network	VH	10	10	150	800					itadmin1		0.27	0.0	MANAGEMENT	2550.0	16950	0.0
	BackUp	Procedure	VH	10	10	200	1200					itadmin1	isLocatedIn: Server 2	0.27	0.0	MANAGEMENT	3800.0	25400	0.0
	BackUp	Procedure	VH	10	10	200	1200					itadmin2	isLocatedIn: Server 2	0.27	0.0	MANAGEMENT	3800.0	25400	0.0
	Access Control	Procedure	VH	10	8	350	1500					itadmin1	isLocatedIn: Server 1	0.27	0.0	MANAGEMENT	4550.0	28850	0.0
	Access Control	Procedure	VH	10	8	350	1500					itadmin2	isLocatedIn: Server 1	0.27	0.0	MANAGEMENT	4550.0	28850	0.0
	Services Data	Data	VH	10	10	0	1000					itadmin1	isLocatedIn: Server 2	0.27	0.0	MANAGEMENT	3000.0	21000	0.0
	Tools Data	Data	VH	10	10	0	1000					itadmin1	isLocatedIn: Server 2	0.27	0.0	MANAGEMENT	3000.0	21000	0.0
	Tools Data	Data	VH	10	10	0	1000					itadmin2	isLocatedIn: Server 2	0.27	0.0	MANAGEMENT	3000.0	21000	0.0

Figure 9 - Outcome of RAOHM

4.1.3 BDCPM - Crawlers

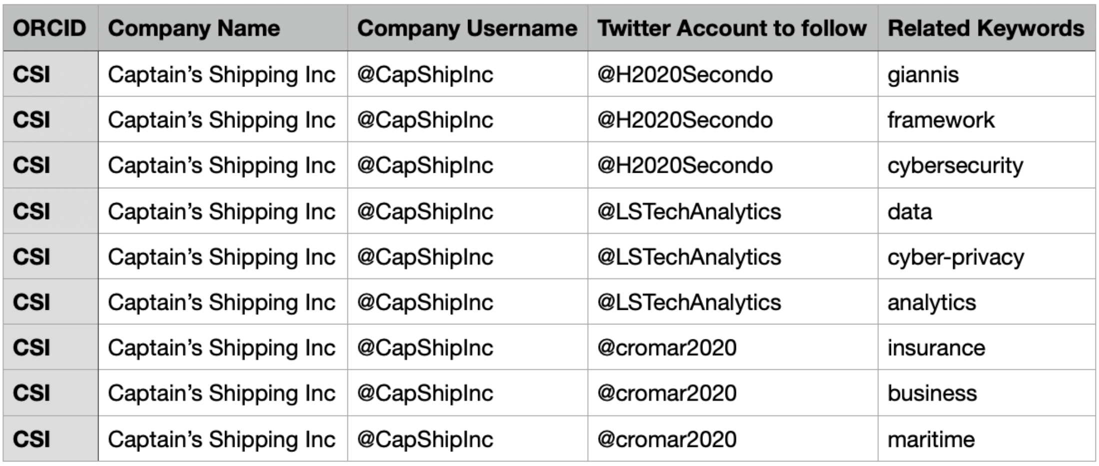
The next step is to set up the input for the Big Data Collection and Processing Module, where the crawlers that are being used should be executed. BDCPM is a standalone component that leverages two specific crawlers, the Twitter, and the Dark Web ones, aiming to retrieve insights. These kinds of insights will be used as input to the final estimation of the premium after the CICPM calculations.

The Twitter crawler requests the following data:

- The ORCID, which is an identifier for the shipping company,
- The company’s name,
- The company’s username in Twitter,

- The Twitter accounts that may follow
- The related keywords, which the crawlers will process.

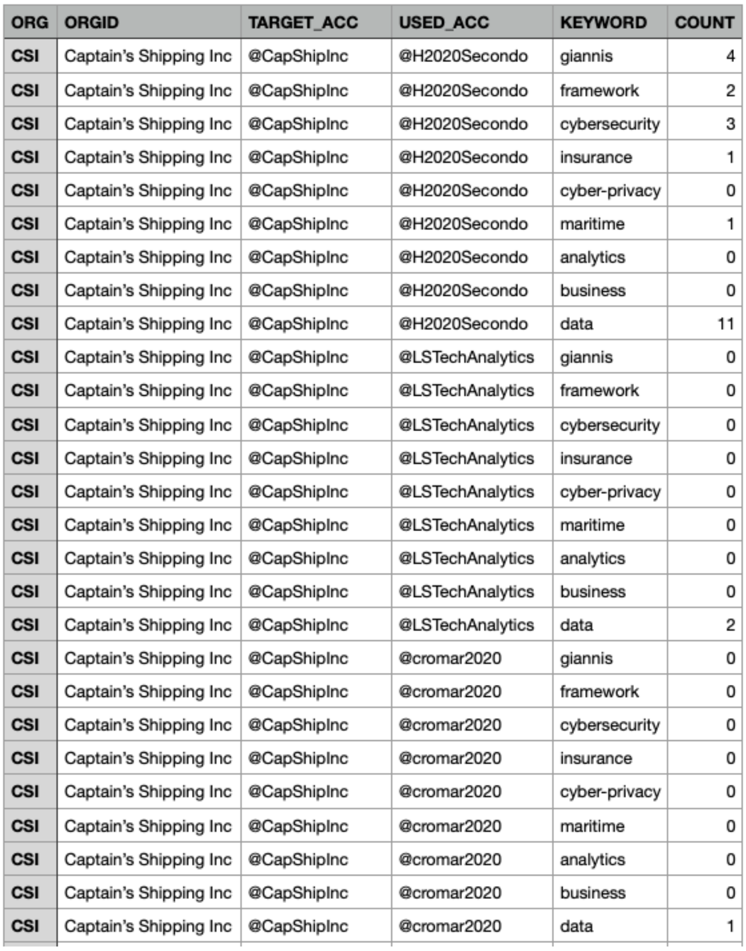
The Twitter crawler input has the csv. file format, and is presented in the following Figure 10:



ORCID	Company Name	Company Username	Twitter Account to follow	Related Keywords
CSI	Captain's Shipping Inc	@CapShipInc	@H2020Secondo	giannis
CSI	Captain's Shipping Inc	@CapShipInc	@H2020Secondo	framework
CSI	Captain's Shipping Inc	@CapShipInc	@H2020Secondo	cybersecurity
CSI	Captain's Shipping Inc	@CapShipInc	@LSTechAnalytics	data
CSI	Captain's Shipping Inc	@CapShipInc	@LSTechAnalytics	cyber-privacy
CSI	Captain's Shipping Inc	@CapShipInc	@LSTechAnalytics	analytics
CSI	Captain's Shipping Inc	@CapShipInc	@cromar2020	insurance
CSI	Captain's Shipping Inc	@CapShipInc	@cromar2020	business
CSI	Captain's Shipping Inc	@CapShipInc	@cromar2020	maritime

Figure 10 - Twitter Crawler input

In the following Figure 11, part of the outcomes of the BDCPM tool are listed, also in csv. file format, where the number of each keyword's appearance is calculated, depending on the Twitter accounts, indicating what relative information is available in Twitter.

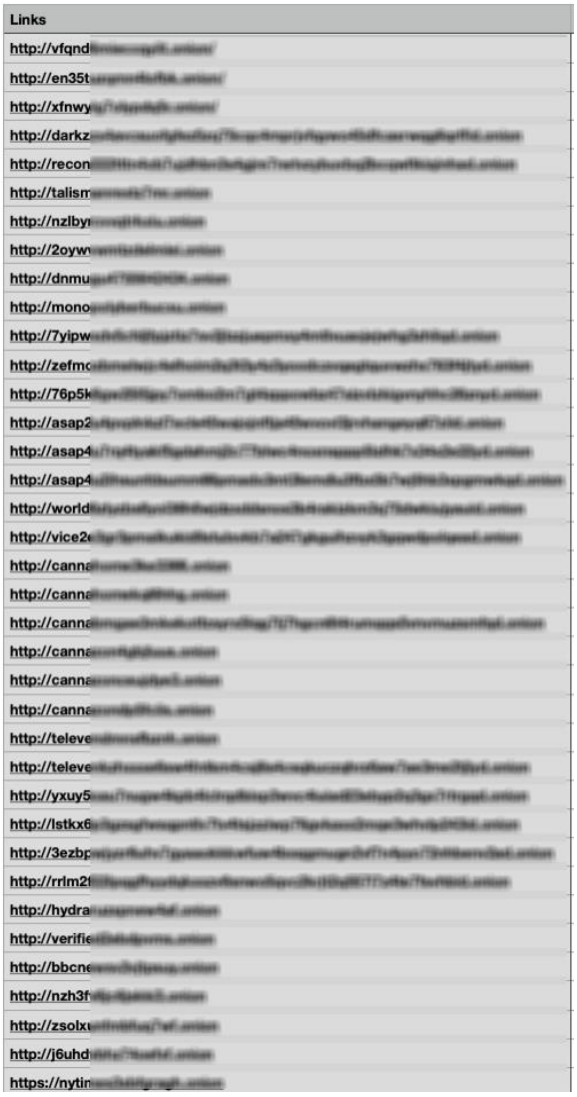


ORG	ORGID	TARGET_ACC	USED_ACC	KEYWORD	COUNT
CSI	Captain's Shipping Inc	@CapShipInc	@H2020Secondo	giannis	4
CSI	Captain's Shipping Inc	@CapShipInc	@H2020Secondo	framework	2
CSI	Captain's Shipping Inc	@CapShipInc	@H2020Secondo	cybersecurity	3
CSI	Captain's Shipping Inc	@CapShipInc	@H2020Secondo	insurance	1
CSI	Captain's Shipping Inc	@CapShipInc	@H2020Secondo	cyber-privacy	0
CSI	Captain's Shipping Inc	@CapShipInc	@H2020Secondo	maritime	1
CSI	Captain's Shipping Inc	@CapShipInc	@H2020Secondo	analytics	0
CSI	Captain's Shipping Inc	@CapShipInc	@H2020Secondo	business	0
CSI	Captain's Shipping Inc	@CapShipInc	@H2020Secondo	data	11
CSI	Captain's Shipping Inc	@CapShipInc	@LSTechAnalytics	giannis	0
CSI	Captain's Shipping Inc	@CapShipInc	@LSTechAnalytics	framework	0
CSI	Captain's Shipping Inc	@CapShipInc	@LSTechAnalytics	cybersecurity	0
CSI	Captain's Shipping Inc	@CapShipInc	@LSTechAnalytics	insurance	0
CSI	Captain's Shipping Inc	@CapShipInc	@LSTechAnalytics	cyber-privacy	0
CSI	Captain's Shipping Inc	@CapShipInc	@LSTechAnalytics	maritime	0
CSI	Captain's Shipping Inc	@CapShipInc	@LSTechAnalytics	analytics	0
CSI	Captain's Shipping Inc	@CapShipInc	@LSTechAnalytics	business	0
CSI	Captain's Shipping Inc	@CapShipInc	@LSTechAnalytics	data	2
CSI	Captain's Shipping Inc	@CapShipInc	@cromar2020	giannis	0
CSI	Captain's Shipping Inc	@CapShipInc	@cromar2020	framework	0
CSI	Captain's Shipping Inc	@CapShipInc	@cromar2020	cybersecurity	0
CSI	Captain's Shipping Inc	@CapShipInc	@cromar2020	insurance	0
CSI	Captain's Shipping Inc	@CapShipInc	@cromar2020	cyber-privacy	0
CSI	Captain's Shipping Inc	@CapShipInc	@cromar2020	maritime	0
CSI	Captain's Shipping Inc	@CapShipInc	@cromar2020	analytics	0
CSI	Captain's Shipping Inc	@CapShipInc	@cromar2020	business	0
CSI	Captain's Shipping Inc	@CapShipInc	@cromar2020	data	1

Figure 11 - Twitter Crawler Outcome

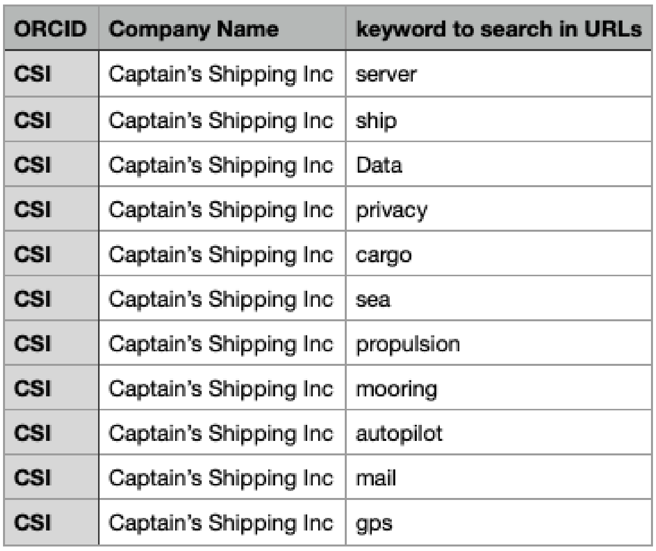
As it is already mentioned above, the SECONDO Platform provides a more special, but also dangerous crawler, that searches the Dark Web.

The Dark Web crawler is fed with two csv. files. The first input file is an extensive list of links that are strongly related to the Dark Web sites (Figure 12). In the second input file, insights in the form of keywords and the shipping company ORCID and name are listed (Figure 13). Thus, through this list the crawler will deep dive to the listed sites, processing the keywords and searching for any kind of information (legal or not), aiming to measure the danger that may affect the shipping company.



Links
http://vfqnd[redacted]
http://en35t[redacted]
http://xfnwy[redacted]
http://darkz[redacted]
http://recon[redacted]
http://talism[redacted]
http://nzlby[redacted]
http://2oyw[redacted]
http://dnmu[redacted]
http://mono[redacted]
http://7yipw[redacted]
http://zefm[redacted]
http://76p5[redacted]
http://asap2[redacted]
http://asap4[redacted]
http://asap4[redacted]
http://world[redacted]
http://vice2[redacted]
http://cann[redacted]
http://cann[redacted]
http://cann[redacted]
http://cann[redacted]
http://cann[redacted]
http://cann[redacted]
http://televe[redacted]
http://televe[redacted]
http://yxuy5[redacted]
http://lstkx6[redacted]
http://3ezbp[redacted]
http://rrlm2[redacted]
http://hydra[redacted]
http://verifi[redacted]
http://bbcn[redacted]
http://nzh3f[redacted]
http://zsolx[redacted]
http://j6uhd[redacted]
https://nytin[redacted]

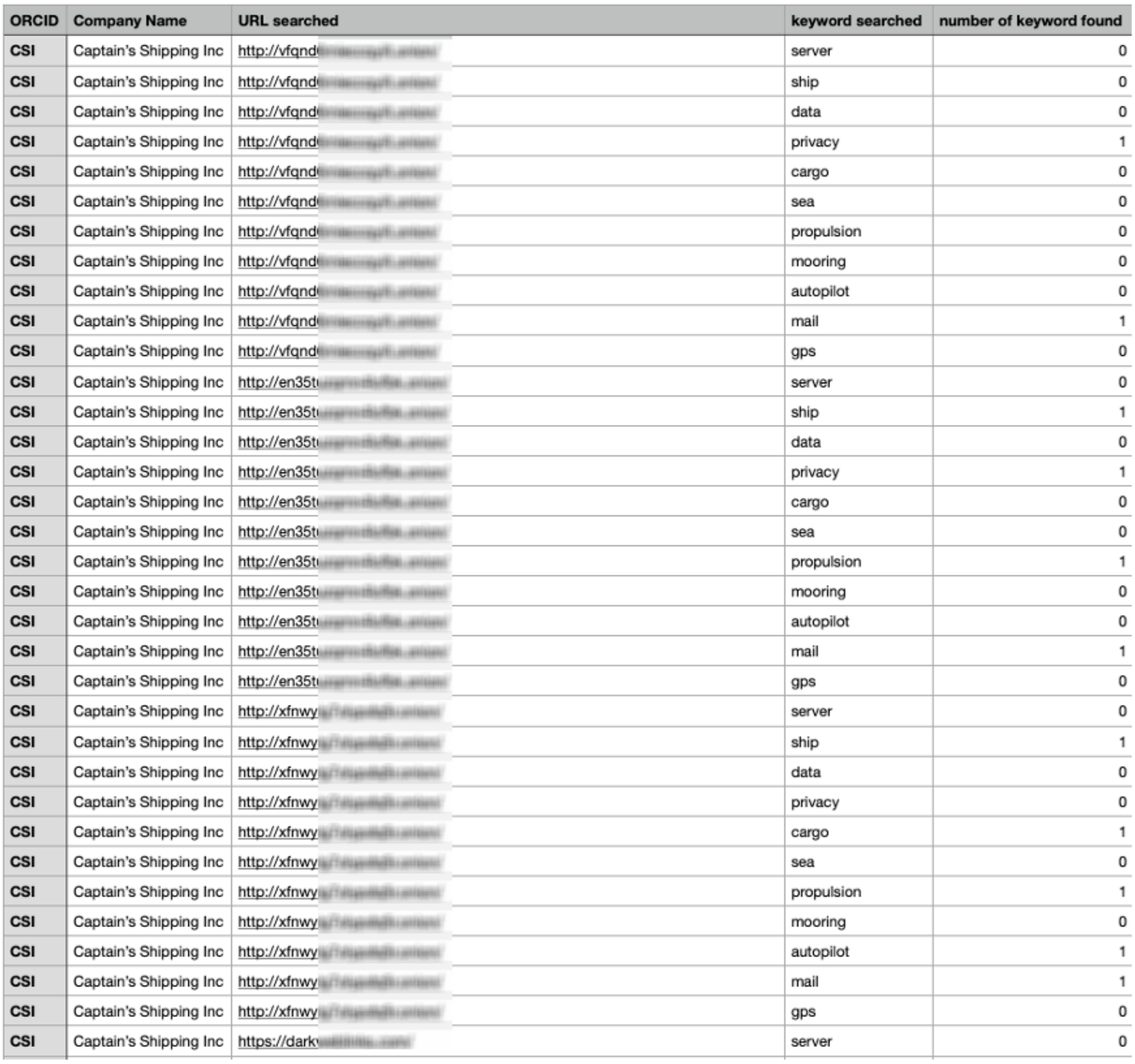
Figure 12 - Dark Web Crawler input links



ORCID	Company Name	keyword to search in URLs
CSI	Captain's Shipping Inc	server
CSI	Captain's Shipping Inc	ship
CSI	Captain's Shipping Inc	Data
CSI	Captain's Shipping Inc	privacy
CSI	Captain's Shipping Inc	cargo
CSI	Captain's Shipping Inc	sea
CSI	Captain's Shipping Inc	propulsion
CSI	Captain's Shipping Inc	mooring
CSI	Captain's Shipping Inc	autopilot
CSI	Captain's Shipping Inc	mail
CSI	Captain's Shipping Inc	gps

Figure 13 - Dark Web Crawler input keywords

In the following Figure 14, part of the outcomes of the Dark Web crawler are listed, also in csv. file format, where the number of each keyword's appearance is calculated, depending on each site, indicating what relative information is available in the Dark Web and it is accessible by every malicious user.



ORCID	Company Name	URL searched	keyword searched	number of keyword found
CSI	Captain's Shipping Inc	http://vfqnd[redacted]	server	0
CSI	Captain's Shipping Inc	http://vfqnd[redacted]	ship	0
CSI	Captain's Shipping Inc	http://vfqnd[redacted]	data	0
CSI	Captain's Shipping Inc	http://vfqnd[redacted]	privacy	1
CSI	Captain's Shipping Inc	http://vfqnd[redacted]	cargo	0
CSI	Captain's Shipping Inc	http://vfqnd[redacted]	sea	0
CSI	Captain's Shipping Inc	http://vfqnd[redacted]	propulsion	0
CSI	Captain's Shipping Inc	http://vfqnd[redacted]	mooring	0
CSI	Captain's Shipping Inc	http://vfqnd[redacted]	autopilot	0
CSI	Captain's Shipping Inc	http://vfqnd[redacted]	mail	1
CSI	Captain's Shipping Inc	http://vfqnd[redacted]	gps	0
CSI	Captain's Shipping Inc	http://en35t[redacted]	server	0
CSI	Captain's Shipping Inc	http://en35t[redacted]	ship	1
CSI	Captain's Shipping Inc	http://en35t[redacted]	data	0
CSI	Captain's Shipping Inc	http://en35t[redacted]	privacy	1
CSI	Captain's Shipping Inc	http://en35t[redacted]	cargo	0
CSI	Captain's Shipping Inc	http://en35t[redacted]	sea	0
CSI	Captain's Shipping Inc	http://en35t[redacted]	propulsion	1
CSI	Captain's Shipping Inc	http://en35t[redacted]	mooring	0
CSI	Captain's Shipping Inc	http://en35t[redacted]	autopilot	0
CSI	Captain's Shipping Inc	http://en35t[redacted]	mail	1
CSI	Captain's Shipping Inc	http://en35t[redacted]	gps	0
CSI	Captain's Shipping Inc	http://xfnwy[redacted]	server	0
CSI	Captain's Shipping Inc	http://xfnwy[redacted]	ship	1
CSI	Captain's Shipping Inc	http://xfnwy[redacted]	data	0
CSI	Captain's Shipping Inc	http://xfnwy[redacted]	privacy	0
CSI	Captain's Shipping Inc	http://xfnwy[redacted]	cargo	1
CSI	Captain's Shipping Inc	http://xfnwy[redacted]	sea	0
CSI	Captain's Shipping Inc	http://xfnwy[redacted]	propulsion	1
CSI	Captain's Shipping Inc	http://xfnwy[redacted]	mooring	0
CSI	Captain's Shipping Inc	http://xfnwy[redacted]	autopilot	1
CSI	Captain's Shipping Inc	http://xfnwy[redacted]	mail	1
CSI	Captain's Shipping Inc	http://xfnwy[redacted]	gps	0
CSI	Captain's Shipping Inc	https://dark[redacted]	server	0

Figure 14 - Dark Web Crawler Outcome

After the completion of the BDCPM crawlers, several cybersecurity analytics and metrics are provided to the CICPM in order to improve the final calculations of the premium.

4.1.4 GTM

In the scope of the Attack Scenario that was described in Section 3.2 and since the main service of the Game Theory Module (GTM) is to create all the possible attacking scenarios, without ignoring the defensive strategies or security controls that may be applied on the shipping company's assets, a simple Attack Graph is presented in the Figure 15.

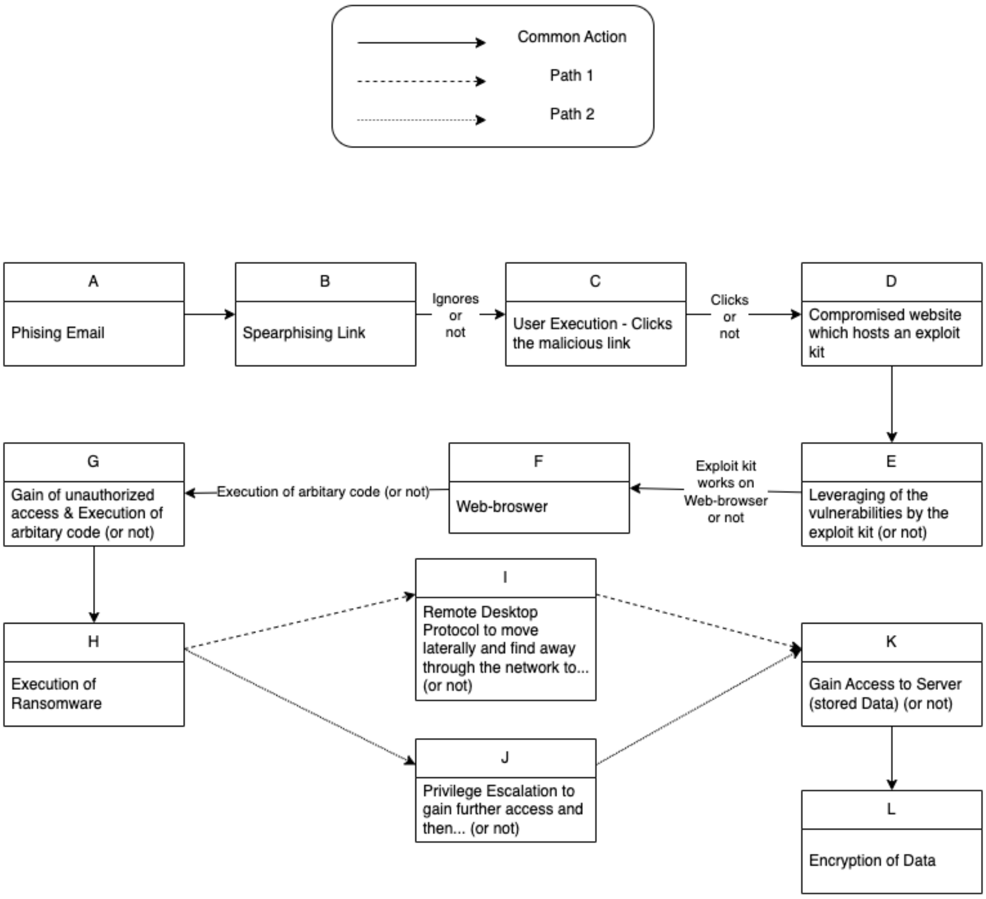

Common Action
Path 1
Path 2
A
Phising Email
B
Spearphising Link
Ignores or not
C
User Execution - Clicks the malicious link
Clicks or not
D
Compromised website which hosts an exploit kit
E
Leveraging of the vulnerabilities by the exploit kit (or not)
Exploit kit works on Web-browser or not
F
Web-broswer
Execution of arbitary code (or not)
G
Gain of unauthorized access & Execution of arbitary code (or not)
H
Execution of Ransomware
I
Remote Desktop Protocol to move laterally and find away through the network to... (or not)
J
Privilege Escalation to gain further access and then... (or not)
K
Gain Access to Server (stored Data) (or not)
L
Encryption of Data

Figure 15 - Attack Graph

Breaking down this Attack Graph, the sequence from a phishing email to ransomware is showcased, providing all the necessary steps in order for the attack to be completed. There is a common path that may be divided into two separate paths, depending on the 2 different types of cyber-attacks (Remote Desktop Protocol & Privilege Escalation) that may be selected by the attacker.

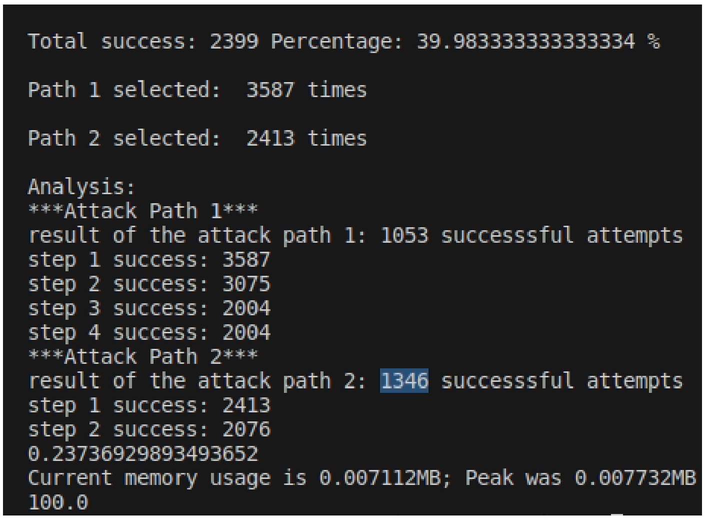
Based on this Attack Scenario and Graph, the actual calculations are implemented using this module.

The first step is to set the budget provided by the shipping company against the cyber threats (1000 monetary units), along with the efficacy on each step of the paths (0,5). Furthermore, it is necessary to set the costs for security controls of each step, aiming to prevent the next one [C(A, B)= 60, C(B, C)= 10, C(C, D)= 5, C(E, F)= 15, C(I, K)= 50, C(J, K)= 60, C(K, L)= 20]. Thus, the next action point is to set the probabilities of the successful steps for all possible paths [P(B, C)= 0.85, P(C, D)= 0.65, P(E,F)= 0.55, P(F, G)= 0.63, P(I, M)= 0.57, P(J, M)= 0.35, P(K, M)= 0.69]. At this point, the module processes the inputs, calculating all the possible attack paths and success percentages.

Table 4: Chosen Security Controls

Control #	Value	Weight	Chosen
1	50	600	No
2	50	100	Yes
3	50	50	Yes
4	50	150	Yes
5	50	500	Yes
6	50	800	No
7	50	200	Yes

The GTM offers two kinds of attack paths calculation, depending on the use of the security controls. The results of the first calculations, without using any security controls, are depicted in the Figure 16, and the calculations' results, where the security controls are included, are shown in the Figure 17.



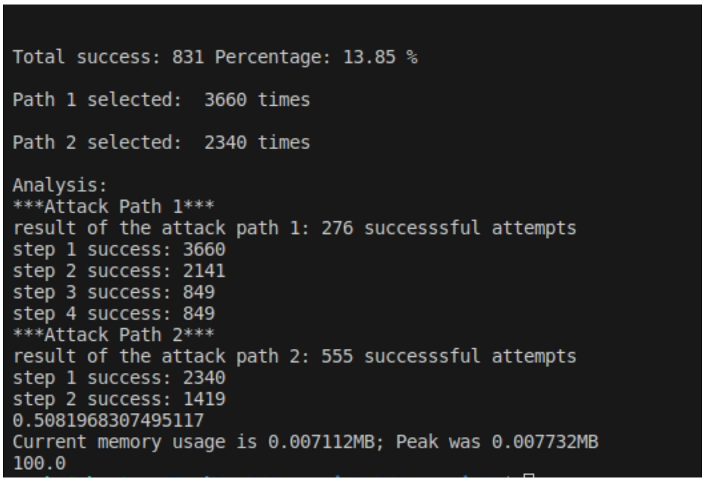
```
Total success: 2399 Percentage: 39.983333333333334 %

Path 1 selected:  3587 times

Path 2 selected:  2413 times

Analysis:
***Attack Path 1***
result of the attack path 1: 1053 successsful attempts
step 1 success: 3587
step 2 success: 3075
step 3 success: 2004
step 4 success: 2004
***Attack Path 2***
result of the attack path 2: 1346 successsful attempts
step 1 success: 2413
step 2 success: 2076
0.23736929893493652
Current memory usage is 0.007112MB; Peak was 0.007732MB
100.0
```

Figure 16 - GTM outcomes without security controls



```
Total success: 831 Percentage: 13.85 %

Path 1 selected:  3660 times

Path 2 selected:  2340 times

Analysis:
***Attack Path 1***
result of the attack path 1: 276 successsful attempts
step 1 success: 3660
step 2 success: 2141
step 3 success: 849
step 4 success: 849
***Attack Path 2***
result of the attack path 2: 555 successsful attempts
step 1 success: 2340
step 2 success: 1419
0.5081968307495117
Current memory usage is 0.007112MB; Peak was 0.007732MB
100.0
```

Figure 17 - GTM outcomes with security controls

In this way, the user of this module is able to extract useful insights, such as the importance and efficiency of the security controls. In the example of the execution, it is obvious that the use of various security controls to different steps is beneficial to the shipping company since there is a significant drop in cyber-attacks (3,8 and 2,42 times down for Attack Path 1 & 2 respectively).

4.1.5 CICPM

The last step is the equation of Premium Calculation that the SECONDO Platform has developed. This equation combines several factors that are outcomes from the abovementioned components, also using insurance-related factors and amounts that are specified in the context of the whole SECONDO Project in order to make more accurate estimations within the total calculation.

Premium = Base Rate (Annual Revenue, Risk Group) * [Down Time Factor] * [Limit of liability factor] * [SECONDO factors] * [Deductible Factor] * [Territory Factor] * [Claims-made Factor] * [Externed Reporting Factor] * [Credit Factor] * [Group Factor] * [Data Factor].

In the following list, there are the amounts and the description of each factor for the use case in order to proceed to the final premium calculation:

i. Base Rate (Annual Revenue, Risk Group):

   a. Annual Revenue: 500.000, which represents the sum of all company's earnings in a year.

   b. Risk Group: 2, which represents the level of risk following the Chubb approach (hazard group categorization) and the 2021 Data Breach Investigations Report (DBIR), by Verizon [23].

ii. Down Time factor: 7, which refers to the hours of the company that its operations are disrupted or unavailable.

iii. Limit of liability factor: 50.000.000, which refers to the maximum amount that an insurance company will pay out for a covered loss or claim under a specific insurance policy. It represents the upper boundary of the insurer's financial responsibility and sets a cap on the amount of compensation that the policyholder can receive.

iv. SECONDO factors, which are related to the framework. There are the Dark Web (20.0) and Twitter (20.0) factors, which use the respective crawlers to include the necessary insights and calculate the factors depending on the number of findings, and the QRAM (60.0) factor which offers the calculation results from the RAOHM, SEAM and BDCPM modules (calculation of the average estimated risk).

v. Deductible factor: 1500, which represents a specified amount of money that the policyholder must pay out of pocket before the insurance coverage kicks in and the insurance company starts paying for covered losses or claims. It is a cost-sharing mechanism between the insured and the insurer.

vi. Territory factor: 1, which refers to the geographical area or region in which the insurance policy's coverage is applicable. It determines the scope of coverage and the locations where the insured events or risks are covered. In this use case is Europe.

vii. Claims-made factor: 1, which represents the type of coverage trigger for liability insurance policies. It specifies that coverage is provided for claims made during the policy period, regardless of when the underlying incident or event causing the claim occurred. In this use case is the 1st year.

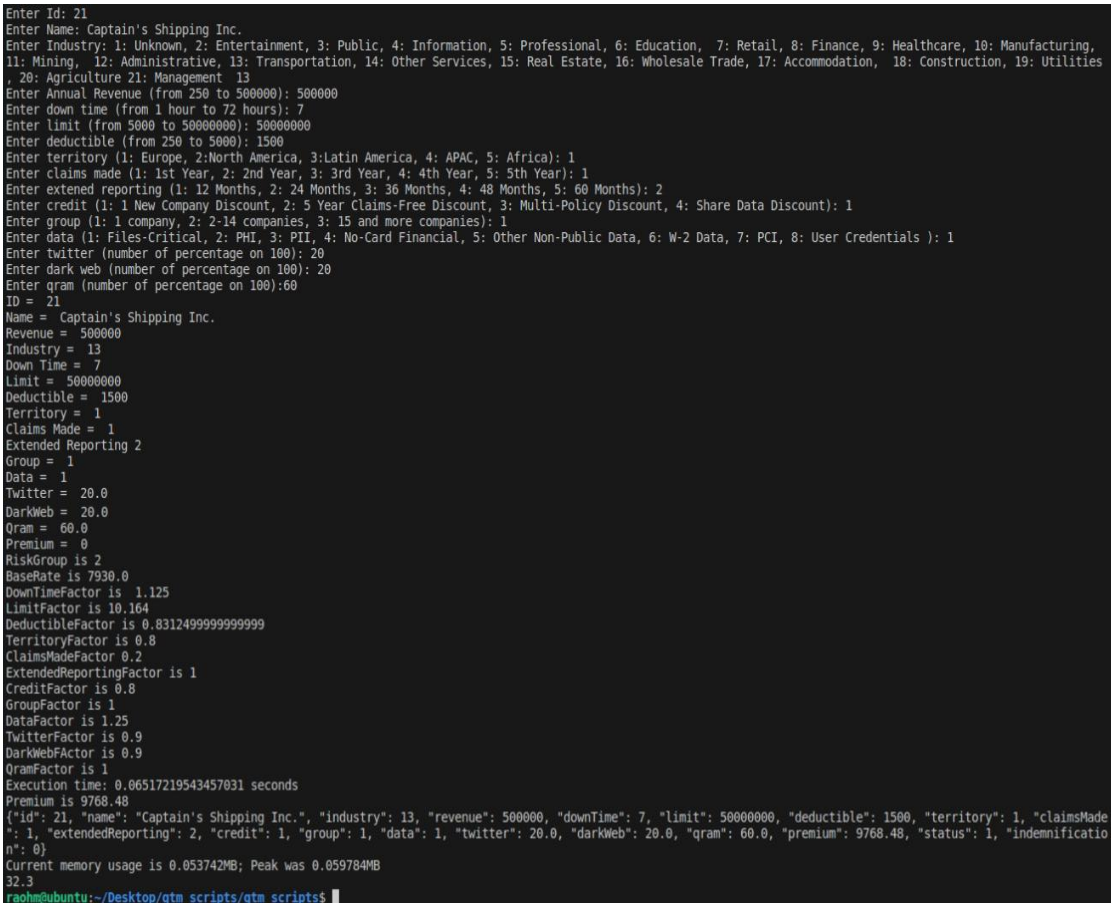
viii. Extended Reporting factor: 2, which represents a provision in insurance policies that allows policyholders to report claims or incidents that occurred during the policy period but are reported after the policy has expired or been canceled. It provides coverage for claims made after the policy's expiration, as long as the incident giving rise to the claim occurred within the specified policy period. In this use case is 24 months.

ix. Credit factor: 0.8, which refers to a numerical rating or score assigned to an individual or business that assesses their creditworthiness. It is used by insurance companies to determine the premium rates for certain types of insurance policies, also providing several types of discounts. In this use case there is a new Company discount.

x. Group factor: 1, which represents the level of insurance of a holding company that owns and insures more than one company under one policy and is considered as group practice. In this use case there is only one company.

xi. Data factor: 1.25, which refers to the type of data that the insured company stores in its infrastructure. In this use case the main types of data are Files-Critical.

Thus, in the following Figure 18 there is the execution and the results of the CICPM module.



```
Enter Id: 21
Enter Name: Captain's Shipping Inc.
Enter Industry: 1: Unknown, 2: Entertainment, 3: Public, 4: Information, 5: Professional, 6: Education,  7: Retail, 8: Finance, 9: Healthcare, 10: Manufacturing,
11: Mining,  12: Administrative, 13: Transportation, 14: Other Services, 15: Real Estate, 16: Wholesale Trade, 17: Accommodation,  18: Construction, 19: Utilities
, 20: Agriculture 21: Management  13
Enter Annual Revenue (from 250 to 500000): 500000
Enter down time (from 1 hour to 72 hours): 7
Enter limit (from 5000 to 50000000): 50000000
Enter deductible (from 250 to 5000): 1500
Enter territory (1: Europe, 2:North America, 3:Latin America, 4: APAC, 5: Africa): 1
Enter claims made (1: 1st Year, 2: 2nd Year, 3: 3rd Year, 4: 4th Year, 5: 5th Year): 1
Enter extened reporting (1: 12 Months, 2: 24 Months, 3: 36 Months, 4: 48 Months, 5: 60 Months): 2
Enter credit (1: 1 New Company Discount, 2: 5 Year Claims-Free Discount, 3: Multi-Policy Discount, 4: Share Data Discount): 1
Enter group (1: 1 company, 2: 2-14 companies, 3: 15 and more companies): 1
Enter data (1: Files-Critical, 2: PHI, 3: PII, 4: No-Card Financial, 5: Other Non-Public Data, 6: W-2 Data, 7: PCI, 8: User Credentials ): 1
Enter twitter (number of percentage on 100): 20
Enter dark web (number of percentage on 100): 20
Enter qram (number of percentage on 100):60
ID =  21
Name =  Captain's Shipping Inc.
Revenue =  500000
Industry =  13
Down Time =  7
Limit =  50000000
Deductible =  1500
Territory =  1
Claims Made =  1
Extended Reporting 2
Group =  1
Data =  1
Twitter =  20.0
DarkWeb =  20.0
Qram =  60.0
Premium =  0
RiskGroup is 2
BaseRate is 7930.0
DownTimeFactor is  1.125
LimitFactor is 10.164
DeductibleFactor is 0.8312499999999999
TerritoryFactor is 0.8
ClaimsMadeFactor 0.2
ExtendedReportingFactor is 1
CreditFactor is 0.8
GroupFactor is 1
DataFactor is 1.25
TwitterFactor is 0.9
DarkWebFActor is 0.9
QramFactor is 1
Execution time: 0.06517219543457031 seconds
Premium is 9768.48
{"id": 21, "name": "Captain's Shipping Inc.", "industry": 13, "revenue": 500000, "downTime": 7, "limit": 50000000, "deductible": 1500, "territory": 1, "claimsMade
": 1, "extendedReporting": 2, "credit": 1, "group": 1, "data": 1, "twitter": 20.0, "darkWeb": 20.0, "qram": 60.0, "premium": 9768.48, "status": 1, "indemnificatio
n": 0}
Current memory usage is 0.053742MB; Peak was 0.059784MB
32.3
raohm@ubuntu:~/Desktop/qtm scripts/qtm scripts$ 
```

Figure 18 - CICPM calculation

As a result, the calculated premium for this use case is 9768.48, which is an acceptable amount, as it is approximately the 5% of the shipping company’s revenue.

5. Conclusion

In today's digital landscape, cybersecurity has emerged as a critical concern for businesses across industries. The increasing reliance on technology and interconnected systems has made organizations vulnerable to cyber threats, highlighting the importance of robust cybersecurity measures. Protecting sensitive data, intellectual property, and maintaining the trust of customers and stakeholders are paramount in a world where cyberattacks can cause significant financial and reputational damage.

As businesses navigate the complex cybersecurity landscape, the significance of cyber insurance cannot be overstated. Cyber insurance provides a financial safety net by mitigating the potential losses associated with cyber incidents. It helps businesses recover from data breaches, ransomware attacks, and other cyber threats by covering expenses such as legal fees, forensic investigations, and customer notification. Furthermore, cyber insurance incentivizes organizations to implement effective cybersecurity measures, as insurers often assess and reward proactive security practices when determining coverage and premiums.

The maritime industry, in particular, faces unique cyber risks due to its reliance on interconnected systems and the potential impact of cyberattacks on vessel operations and port infrastructure. The attack scenario involving the ransomware attack on the shipping company, Captain’s Shipping Inc, exemplifies the devastating consequences such attacks can have on maritime operations. Cyber-insurance plays a crucial role in mitigating financial losses and facilitating the recovery process for shipping companies in the event of a cyber incident.

The SECONDO Project, with its various modules, offers a comprehensive approach to enhancing cybersecurity. The Social Engineering Assessment Module, Risk Analysis Ontology and Harmonization Module, Big Data Collection and Processing Module, Game Theory Module, and Cyber Insurance Coverage and Premiums Module collectively provide valuable insights and tools for organizations to assess risks, detect vulnerabilities, and implement proactive security measures, along with the cyber-insurance aspect and the calculation of premiums.

Further exploitation and research in the field of cybersecurity are vital to stay ahead of evolving threats. Ongoing research can focus on developing advanced detection and response mechanisms, refining cyber-insurance models to accurately assess risk and premiums, and exploring emerging technologies such as artificial intelligence and blockchain to bolster cybersecurity measures. Collaborative efforts between academia, industry, and policymakers can foster innovation and ensure the continual improvement of cybersecurity practices in an increasingly interconnected world.

In conclusion, cybersecurity is of paramount importance across industries, and cyber insurance serves as a critical component in risk management strategies. The maritime industry, with its unique vulnerabilities, necessitates robust cyber-insurance solutions. The SECONDO Project's modules provide valuable tools for organizations to enhance their cybersecurity posture. Continued research and exploration are key to addressing emerging threats and ensuring the resilience of businesses in the face of evolving cyber risks.

References

[1] "About Enisa - the European Union Agency for Cybersecurity." *ENISA*, 20 Apr. 2022, https://www.enisa.europa.eu/about-enisa .

[2] Das, Yashi. "What Is Insurance: Definition, Benefits, and Types." *A Comprehensive Guide to Money Transfer, Recharges, Bill Payments and Other Digital Payments | Paytm Blog*, 9 Nov. 2022, https://paytm.com/blog/insurance/what-is-insurance-definition-benefits-and-types/ .

[3] *A Security Economics Service Platform for Smart Security ... - Europa*. https://cordis.europa.eu/project/id/823997 .

[4] Farao, A., Panda, S., Menesidou, S. A., Veliou, E., Episkopos, N., Kalatzantonakis, G., ... & Xenakis, C. (2020). SECONDO: A platform for cybersecurity investments and cyber insurance decisions. In Trust, Privacy and Security in Digital Business: 17th International Conference, TrustBus 2020, Bratislava, Slovakia, September 14–17, 2020, Proceedings 17 (pp. 65-74). Springer International Publishing.

[5] "Horizon 2020." *Horizon 2020 - European Commission*, https://wayback.archive-it.org/12090/20220124075100/https:/ec.europa.eu/programmes/horizon2020/ .

[6] "D2.1 - Technical Requirements, Business Cases and Reference Architecture." *H2020 SECONDO - A Security ECONomics Service Platform for Smart Security Investments and Cyber Insurance Pricing in the beyonD 2020 NetwOrking Era*, Grant Agreement ID: 823997, 14 Jan. 2020, https://secondo-h2020.eu/wp-content/uploads/2021/04/D2.1_Technical_Requirements_Business_Cases_and_Reference_Architecture.pdf .

[7] "What Is 'Social Engineering'?" *ENISA*, 29 Nov. 2022, https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering .

[8] "The CORAS Method." *The CORAS Method*, https://coras.sourceforge.net/ .

[9] Kalderemidis, I., Farao, A., Bountakas, P., Panda, S., & Xenakis, C. (2022, August). GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-9).

[10] Karatisoglou, M., Farao, A., Bolgouras, V., & Xenakis, C. (2022, June). BRIDGE: BRIDGing the gap bEtween CTI production and consumption. In 2022 14th International Conference on Communications (COMM) (pp. 1-6). IEEE.

[11] Charalambous, M., Farao, A., Kalantzantonakis, G., Kanakakis, P., Salamanos, N., Kotsifakos, E., & Froudakis, E. (2022, August). Analyzing Coverages of Cyber Insurance Policies Using Ontology. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-7).

[12] Capano, Daniel E. "Throwback Attack: How Notpetya Accidentally Took down Global Shipping Giant Maersk." Industrial Cybersecurity Pulse, 15 Aug. 2022, https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/ .

[13] Team, Port Technology. "Cosco Fights on against Cyberattack." *Port Technology International*, 27 July 2018, https://www.porttechnology.org/news/cosco_fights_on_against_cyberattack/ .

[14] Grove, Jennifer Van. "Port of San Diego Victim of Cyberattack." *Tribune*, San Diego Union-Tribune, 27 Sept. 2018, https://www.sandiegouniontribune.com/business/growth-development/sd-fi-port-cyberattack-20180926-story.html .

[15] "Vard Shipbuilder Experiences Ransomware Attack." *SAFETY4SEA*, 11 June 2020, https://safety4sea.com/vard-shipbuilder-experiences-ransomware-attack/ .

[16] "Shen Attack Cyber Risk in Asia Pacific Ports - Lloyd's." *Shen Attack Cyber Risk In Asia Pacific Ports - Lloyd's*, 12 Oct. 2019, https://www.lloyds.com/news-and-insights/risk-reports/library/shen-attack-cyber-risk-in-asia-pacific-ports .

[17] "Marine Cyber Risk and Insurance: Howden." *Howden United Arab Emirates*, 11 June 2021, https://www.howdengroup.com/ae-en/marine-cyber-risk-and-insurance-howden#:~:text=CL380%20%2D%20Institute%20Cyber%20Attack%20Exclusion%20Clause&text=The%20clause%20excludes%20cover%20where,there%20is%20a%20cyber%20attack .

[18] Panda, S., Farao, A., Panaousis, E., & Xenakis, C. (2021). Cyber-Insurance: Past, Present and Future. In Encyclopedia of Cryptography, Security and Privacy (pp. 1-4). Berlin, Heidelberg: Springer Berlin Heidelberg.

[19] "Understanding Data Breach and Cyber Liability Coverage." *Understanding Data Breach and Cyber Liability Coverage | The Hanover Insurance Group*, www.hanover.com/resources/tips-individuals-and-businesses/prepare-now-learn-how/understanding-data-breach-and-cyber . Accessed 11 May 2023.

[20] "The Modern Day Blackmail: Understanding the Dangers of Cyber Extortion." *Dataconomy*, 22 Dec. 2022, https://www.dataconomy.com/2022/12/20/cyber-extortion-examples-types-and-laws/#:~:text=Cyber%20extortion%20refers%20to%20the%20use%20of%20various%20tactics%2C%20such,of%20different%20types%20of%20cybercrime .

[21] “Business Interruption in a Cyber Policy.” *Insurance Training Center*, 21 Dec. 2022, https://www.insurancetrainingcenter.com/resource/business-interruption-in-a-cyber-policy/ .

[22] Dan BurkeSenior Vice President, Cyber Practice LeaderEditor. “Cyber 101: Understand the Basics of Cyber Liability Insurance.” *Woodruff Sawyer*, 30 Jan. 2023, https://www.woodruffsawyer.com/cyber-liability/cyber-101-liability-insurance/ .

[23] “Cybercrime Thrives during Pandemic: Verizon 2021 Data Breach Investigations Report.” *Verizon*, 20 May 2021, www.verizon.com/about/news/verizon-2021-data-breach-investigations-report .