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

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

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

SECONDO

WP2 – Requirements, Business Cases and Architecture

Deliverable D2.1 "Technical Requirements, Business Cases and Reference Architecture"

Editor(s):	Christos Xenakis (UPRC)
Author(s):	Christos Xenakis (UPRC), Farnaz Mohammadi(UPRC), George Kalantzantonakis(LST), Dimitrianos Savva (LST), Evangelos Kotsifakos (LST), Nikolaos Georgopoulos (CRO), Sirivianos Michael (CUT), Michael Pingos (CUT), Nikos Salamanos (CUT), Spyridonas Loizou (CUT), Nikolaos Episkopos (FOGUS), Emmanouil Panaousis (UoG), Sakshyam Panda (SUR), Sofia Anna Menesidou (UBI), Entso Veliou (UBI)
Dissemination Level:	PU - Public
Type:	R - Report
Version:	2.3

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

Partners

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

Document History

VERSIONS

Version	Date	Author	Remarks
0.1	23/10/2019	UPRC	Table of Content
0.2	28/11/2019	UPRC	UPRC-SOTA-QRAM
0.3	09/12/2019	CRO	CRO-SOTA- Cyber Insurance-Smart contract
0.4	7/12/2019	CUT	Technical Requirements
0.5	15/12/2019	UBI	Reference platform Architecture
0.6	15/12/2019	SUR.	State-of-the-art
0.7	15/12/2019	SUR, FOGUS, LSTECH	Business Case 1,2, 3
0.8	15/12/2019	CRO	Business Case 4
1	17/12/2019	UPRC	First Draft
1.1	20/12/2019	ALL	Review
1.2	27/12/2019	UBI	Revised Reference Platform Architecture
1.3	29/12/2019	UBI	Inputs and outputs between SECONDO components and modules
1.4	30/12/2019	CUT	Revised Requirements
1.5	4/1/2020	CRO	Revised Business Case 4
2	7/1/2020	UPRC	Second Draft
2.1	10/1/2020	ALL	Review
2.2	13/1/2020	CRO	Revised version of Business Case 4
2.3	14/1/2020	UPRC	Final Version

Executive Summary

The overall aim of SECONDO is to make impact on the operation of EU businesses who often: (i) have a limited cyber security budget; and (ii) ignore the importance of cyber insurance. Cyber insurance can play a critical role to the mitigation of cyber risk. This can be done by imposing a cost on firms' cyber risk through a premium that they have to pay. Firms can then improve on their cyber security investments reducing their cyber security risks so that they are eligible to receive a smaller cyber insurance premium. SECONDO will offer a software platform to address the above matter narrowing the gap between theoretical understanding and practice.

Deliverable 2.1 is dedicated to the documentation of the work done in the three tasks in WP2, which are detailed below.

Task 2.1: "Business cases and specifications". SECONDO beneficiaries collected, selected and assembled detailed information from user groups (mainly existing customers) to define users, usage, and business requirements of the SECONDO platform. The business cases cover specific aspects of the project, such as risk modelling, cyber security investment decisions and cyber insurance in end users of different sizes or types. Emphasis will be given on the specification of requirements that are derived from existing limitations of current risk analysis methodologies that deteriorate the decisions on optimal investments in cyber security and cyber insurance.

Task 2.2: "Technical requirements specification". This task translates the operational needs of SECONDO stakeholders to technological requirements. The list of business requirements defined in Task 2.1 will be analysed, to define whether they are unclear, incomplete, ambiguous, or contradictory to the business scenarios.

Task 2.3: "Reference platform architecture". This task provides the abstract reference architecture of the SECONDO platform. Primary drivers of the architecture's definition will be the functional and non-functional requirements as produced in previous tasks of WP2.

Table of Contents

Executive Summary 4
Table of Figures 7
Table of Tables 8
Abbreviations 9

1 Introduction 11
1.1 A brief description of the SECONDO project 11
1.2 Role of the Deliverable 12
1.3 Relationship to other Deliverables 12
1.4 Structure of the document 13

2 State of the art 13
2.1 Quantitative Risk Analysis Metamodel 13
2.1.1 QRAS 16
2.1.2 Game Theoretic Module (GTM) 16
2.1.3 Continuous Risk Monitoring Module (CRMM) 17
2.1.4 Social Engineering Assessment Module (SEAM) 18
2.1.5 Attack Graph 18
2.1.6 Bayesian Networks 19
2.2 Optimal Investment in Cyber Security Blockchain 19
2.2.1 Cyber Security Investments 20
2.2.2 Blockchain in Cyber Insurance 23
2.3 Cyber Insurance and Smart Contracts 24
2.3.1 Cyber Insurance 24
2.3.2 Smart Contracts 26

3 General Insurance Challenges 28

4 Cyber Security Incidents 30

5 Use Cases 31
5.1 Introduction 31
5.2 Methodology 32
5.3 Terminology 33
5.3.1 Participating modules 33
5.4 Use Case 1 – Human susceptibility to cybersecurity breaches in IoT-enabled smart home 33
5.4.1 Use Case Motivation 33
5.4.2 Scenario 34
5.5 Use Case 2 – Optimal Patching of Airport Cyber Infrastructures 35
5.5.1 Motivation 35
5.5.2 Scenario 35
5.6 Use Case 3 – Cyber insurance for Innovative SME 35
5.6.1 Motivation 35
5.6.2 Scenario 36

5.7 Use Case 4 - Cyber Risk Transfer in Maritime Industry 36
5.7.1 Motivation 36
5.7.2 Hull Cyber Cover 38
5.7.3 Attack Timeline 42

6 Technical Requirements Specification 43
6.1 Quantitative Risk Analysis Metamodel (QRAM) 43
6.2 Risk Analysis Ontology and Harmonisation Module (RAOHM) 44
6.3 Social Engineering Assessment Module (SEAM) 46
6.4 Cyber Security Investment Module (CSIM) 47
6.5 Game Theoretic Module (GTM) 48
6.6 Econometrics Module (ECM) 50
6.7 Continuous Risk Monitoring Module (CRMM) 51
6.8 Cyber Insurance Coverage and Premiums Module (CICPM) 53
6.9 Big Data Collection and Processing Module (BDCPM) 54

7 Reference Platform Architecture 55
7.1 Quantitative Risk Analysis Metamodel (QRAM) 59
7.1.1 Social Engineering Assessment Module (SEAM) 59
7.1.2 Risk Analysis Ontology and Harmonisation Module (RAOHM) 60
7.2 Big Data Collection and Processing Module (BDCPM) 61
7.3 Continuous Risk Monitoring Module (CRMM) 61
7.4 Cyber Security Investment Module (CSIM) 62
7.4.1 Game Theoretic Module (GTM) 62
7.4.2 Econometrics Module (ECM) 63
7.5 Cyber Insurance Coverage and Premiums Module (CICPM) 64
7.6 Blockchain and Smart Contracts 64

8 Candidate Implementation Technologies 65
8.1 Blockchain and Smart Contracts 66
8.2 Risk Managements (Modelling and Analysis) 68
8.3 Data Processing and ELK Stack 70
8.4 SECONDO Platform Implementation 71

9 Conclusions 71

10 References 72

Table of Figures

Figure 1 Workflow of setting up a Game Theoretic Model [14] 17
Figure 2 General Insurance Challenges 30
Figure 3 - Risk Transfer with SECONDO 39
Figure 4 - Incident Response with SECONDO 41
Figure 5 SECONDO High Level Architecture 56
Figure 6 SECONDO Technologies 66
Figure 7 SECONDO Technologies 67
Figure 8 CORAS security risk analysis steps 68
Figure 9 The CORAS framework for model-based risk assessment 69
Figure 10 OLISTIC Results 70
Figure 11 ELK 71

Table of Tables

Table 1 Abbreviations 9

Table 2 Differences between the Standard Hull and Machinery Insurance and the standard Cyber Insurance 38

Table 3 QRAM Requirements 43

Table 4 RAOHM Requirements 44

Table 5 SEAM Requirements 46

Table 6 CSIM Requirements 47

Table 7 GTM Requirements 48

Table 8 ECM Requirements 50

Table 9 CRMM Requirements 51

Table 10 CICPM Requirements 53

Table 11 BDCPM Requirements 54

Table 12 Inputs and outputs between SECONDO components and modules 56

Table 13 Input/output SEAM 60

Table 14 Input/output RAOHM 61

Table 15 Input/output BDCPM 61

Table 16 Input/output CRMM 62

Table 17 Input/output GTM 63

Table 18 Input/output ECM 64

Table 19Input/output CICPM 64

Table 20 Input/output Blockchain 65

Table 21 Technologies per component 65

Abbreviations

Table 1 Abbreviations

Abbreviation	Meaning
QRAM	Quantitative Risk Analysis Metamodel
RAOHM	Risk Analysis Ontology and Harmonisation Module
SEAM	Social Engineering Module
CSIM	Cyber Security Investment Module
CRMM	Continuous Risk monitoring Module and private blockchain
ECM	Econometrics Module
GTM	Game Theoretic Module
CICPM	Cyber Insurance Coverage and Premium Module
SC	Smart Contract
INS	Insurance company
WP	Work Package
NE	Nash Equilibria
SME	Small and Medium sized Enterprises
DRT	Disaster Recovery Team
BRT	Business Recovery Team
PR	Personal Relations
IoT	Internet of Things
UML	Unified Modeling Language
MULVAL	Multihost, Multistage, Vulnerability Analysis
TVA	Topological Vulnerability Analysis
MOTS	Multi-Objective Tabu Search
GA	Genetic Algorithm
BF	Brute Force
DAG	Directed Acyclic Graph
CPT	Conditional Probability Table

1 Introduction

The following pages provide a brief overview on the overall goals of the SECONDO project and a description of the scope of this deliverable together with an outlook on the further steps for the overall analysis of the SECONDO solution.

1.1 A brief description of the SECONDO project

In order for the SECONDO platform to achieve the highly accurate calculations of optimal security investments and cyber insurance premiums, the following limitations must first be addressed

- Asset interdependencies: the interdependencies of security vulnerabilities and the multidisciplinary nature of cyber threats is a problem that does not only exhibits technological dimensions. It has to be carefully studied, analyzed and understood from societal, organization, regulatory and economic points of view.

- Growing and evolving types of impact: the rapidly changing cyber landscape, which implies that historical data may not reflect the most recent risk levels. Hence, it is not possible for decision-makers and insurers to use traditional approaches to model loss distribution and perform accurate risk assessment.

- Quantifying cyber risks: the lack of verified and standardised risk management methodologies that employ commonly agreed metrics and risk aggregators aiming to provide quantitative results that apply to both tangible (e.g. property) and intangible (e.g. reputation) assets and methods to price them.

- Growing attack surface: technological inventions and modern paradigms that bring a new range of threats to both tangible and intangible assets. Most of these assets are not covered by established insurance policies, leaving organizations exposed to serious impacts of cyber risks.

- Security economics: the absence of effective applied econometric models that: a) guide and estimate the optimal investment in cyber security solutions and controls to mitigate the estimated risks; and b) compute optimal thresholds of residual risks that must be outsourced to a cyber insurer;

- Knowing the actual losses: the currently limited availability of established methods that can quantify the economic value of an insured organization's information loss and the general unwillingness on the part of companies to share such information;

- More inclusive cyber insurance: the role of an insurer as someone that merely protects is not the case anymore, given that clients demand preventative solutions to stop cyber incidents before damage is inflicted and they also ask for support during a crisis to avoid the penalization of their businesses.

SECONDO will provide a scalable, highly interoperable Economics-of-Security-as-a-Service (ESaaS) platform that encompasses a comprehensive cost-driven methodology for: (i) estimating cyber risks based on a quantitative approach that focuses on both technical and non-technical aspects, (e.g. users

behavior), that influence cyber exposure; (ii) providing analysis for effective and efficient risk management by recommending optimal investments in cyber security controls; and (iii) determining the residual risks and estimating the cyber insurance premiums taking into account the insurer's business strategy, while eliminating the information asymmetry between the insured and insurer.

1.2 Role of the Deliverable

The role of this deliverable is to provide a description of the use cases, technical requirements as well as reference architecture of the SECONDO, therefore establishing a full set of specifications that will serve to implement the system.

The present document has two main purposes:

- Describe the use cases and technical requirements of the SECONDO system.
- Serve as a reference for other deliverables on how to implement the SECONDO system.

1.3 Relationship to other Deliverables

D2.1 provides the first rough sketch of SECONDO setting the platform on which the Econometric Module (ECM) will be provided, the Continuous Risk monitoring Module and private blockchain (CRMM) in conjunction with a blockchain implementation to register the monitored risk level and create smart contracts, the CSIM that is empowered by the Game Theoretic and EM modules will be designed and implemented (WP3); the SECONDO Cyber Insurance Ontology, the Cyber Insurance and Premiums Modules, and the Cyber Insurance Smart Contract will be developed (WP4); . The definition of the technical integrated endpoints and proactive planning of the integration of the SECONDO modules developed in previous work packages (WP5); integration, technical testing, assessment of the platform in real-life use cases and refinement of the SECONDO prototype (WP6); As such, D2.1 is linked to all the major deliverables of the project.

- D3.1 : Pricing Methods and Risk Modelling – The RAOHM module as part of the SECONDO ecosystem has to respect the scenarios defined in Section 5 and the architecture described in Section 6 of this D2.1.

- D3.2 : Big Data Collection and Processing – The BDCPM module that acquires risk related data either from internal organizational sources or external sources will respect the scenarios defined in Section 5 and the architecture described in Section 6 of this D2.1.

- D4.1 : Econometrics – The e Econometrics Module (ECM) that provides estimates of all kinds of costs of potential attacks as well as costs will respect the scenarios defined in Section 5 and the architecture described in Section 6 of this D2.1.

- D4.2 : Continuous Risk Monitoring and Blockchain – The CRMM module will assess on a continuous basis the risk levels, including the performance of the implemented cyber security controls will respect the scenarios defined in Section 5 and the architecture described in Section 6 of this D2.1.

- D4.3 : Cyber Security Investments – The CSIM module that will be responsible for inferring optimal investment plans will respect the scenarios defined in Section 5 and the architecture described

in Section 6 of this D2.1.

- D5.1 : Cyber Insurance Market, Attributes and Sources – The comprehensive survey and analysis of the cyber insurance market and well-known insurance policies that will be provided will respect the scenarios defined in Section 5 and the architecture described in Section 6 of this D2.1.

- D5.2 : Cyber Insurance Policy Ontology – The provided ontology that will provide a common vocabulary and language of the cyber insurance policies will respect the scenarios defined in Section 5 and the architecture described in Section 6 of this D2.1.

- D5.3 : Decision Support for Cyber Insurance - The CICPM that will provide insurance exposure assessment and estimate insurance coverage and premiums, will respect the scenarios defined in Section 5 and the architecture described in Section 6 of this D2.1.

- D6.1 & D2: Platform Integration and Platform Assessment - The system described in D6.1 & D6.2 will respect the technical requirements specified in Section 6 of this D2.1.

In addition, all mentioned deliverables will use the candidate technologies that are described in section 5 of this deliverable.

1.4 Structure of the document

Chapter 2 provides the state-of-the-art, SECONDO will go beyond the state-of-the-art by integrating many different techniques.

Chapter 3 demonstrates the challenges which SECONDO has to cope in order to achieve its goals.

Chapter 4 analyses some cyber security incidents that affected well-known companies and there were issues with their insurers.

Chapter 5 performs the high-level requirements analysis through four (4) use cases, their scenarios, and the modules which interact within the SECONDO platform.

Chapter 6 provides the technical requirements.

Chapter 7 provides a description of the SECONDO reference platform to be used in the future development of the project.

Finally, Chapter 8 specifies some candidate implementation technologies and algorithms for achieving the SECONDO outcome.

2 State of the art

In this section, we will present the state-of-the-art for each of the modules comprising the SECONDO platform: a) Quantitative Risk Analysis Metamodel; b) Optimal Investment in Cyber Security and Blockchain and c) Cyber Insurance and Smart Contracts.

2.1 Quantitative Risk Analysis Metamodel

Risk analysis is one of the fundamental components of an organizational risk management process.

The purpose of risk analysis is to inform decision makers and support risk responses by identifying: a) relevant threats to organizations or threats directed through organizations against other organizations; b) vulnerabilities both internal and external to organizations (i.e. asset, service, business process); c) impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and d) likelihood that harm will occur; d) The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring) [1] [2].

Many methodologies have been developed to undertake a risk analysis of an industrial plant. In order to understand their running, it is necessary to examine the input data, methods used, obtained output data and to rank them in several classes. The review of existing methodologies considers not only current European standards but also national standards, guidelines and current practices. In principle, a risk assessment methodology needs to consider all risk factors, including unexpected parameters. For example, the methodology needs to answer the following fundamental questions : a) What is the risk? b) Do we have an incident waiting to happen? c) What can go wrong/What are the potential consequences? d) What is the chain of events which could lead to harm? e) Can we tolerate the potential consequences at the estimated likelihood? f) What are the benefits and costs of alternative technologies? etc.

In addition, a probabilistic relational model makes it possible to associate a probabilistic dependency model to the attributes of classes in the architectural metamodel. A probabilistic relational model contains classes, attributes, and class-relationships. It can be used to specify architectural metamodels similar to class diagrams in the Unified Modeling Language (UML). [3] proposes a set of abstract classes that can be used to create probabilistic relational models to enable inference of security risk from instantiated architecture models.

Qualitative and quantitative analysis are two fundamental methods of interpreting data in research. Moreover, there are overlaps in quantitative and qualitative analysis. The main differences between quantitative and qualitative research consist in respect to data sample, data collection, data analysis, and last but not least in regard to outcomes. Qualitative analysis fundamentally means to measure something by its quality rather than quantity, while Quantitative analysis is often associated with numerical analysis where data is used for specific findings using a set of statistical methods. Quantitative analysis is generally concerned with measurable quantities such as weight, length, temperature, speed, width, and many more. The data can be expressed in a tabular form or any diagrammatic representation using graphs or charts.

According to [4], information security management must start with a quantitative risk analysis. The challenge is that most theoretic approaches to quantitative risk analysis do not work in practical scenarios. The main advantage of a quantitative method is that it considers frequency and severity together in a more comprehensive and sophisticated way than other methods. The main problem is that it can be complicated to obtain data on risks: hazard, exposure, vulnerability and consequential severity. If it is difficult to understand and represent the characteristics of a single risk, then it is even harder to understand their interdependencies. Moreover, another advantage of quantitative analysis is that the findings can be applied in a general population using research patterns. Quantitative data can be classified as continuous or discrete, and it works of literature using surveys, observations,

experiments or interviews.

In seminal work [5], the authors have proposed a security ontology framework that consists of four parts. The first part is the security and dependability taxonomy (an ontology in the form of a hierarchy) [6]; the second part presents the underlying risk analysis methodology; the third part describes concepts of the IT infrastructure; and the fourth part provides a simulation enabling analysis of various strategy scenarios, similarly to what authors have proposed in [7].

It should be noted that in 2017, ENISA published the Threat Landscape Report 2017 [8], which highlighted that incidents in the cyber threat landscape have led to the definitive recognition of some omnipresent facts. On the other hand, security metrics can be used to offer a quantitative and objective basis for security assurance, therefore, facilitating business and engineering decisions concerning information security. Measuring security by obtaining enough evidence in order to make informed decisions is one of the significant challenges in the area of quantitative risk analysis. Currently, there is a plethora of emerging security metrics proposed by academia, government and industry. Some security standards, including ISO/IEC 27004:2009, ISO/IEC 21827, SSE-CMM and NIST SP 800-55, use the same metrics in different ways; thus, existing standards are not fully harmonised.

One of the critical contributions of the SECONDO programme in the area will be the design, analysis and implementation of a Quantitative Risk Analysis Metamodel (QRAM) that will utilise advanced security metrics to quantitatively estimate the exposed cyber risks, taking into account essential parameters not currently considered by existing risk analysis tools. SECONDO will also define advanced methodologies for digital asset identification and valuation. Qualitative and quantitative methods derived both from Business Impact Analysis, and insurance pricing models will be investigated in order to calculate the relative and intrinsic value of an organisation's digital assets.

Nowadays, it is quite common to manage projects with the use of digitally collected data. The Big Data analysis can enhance the quality of information taken from these records and be used for project management. An accurate analysis of all that data Big Data makes it possible to discover new phenomena characteristic for the project. On the one hand, Big Data unleashes tremendous benefits not only to individuals but also to communities and society at large, including breakthroughs in health research, sustainable development, energy conservation and personalized marketing. On the other hand, big data introduces new privacy and civil liberties concerns, including high-tech profiling, automated decision-making, discrimination, and algorithmic inaccuracies or opacities that strain traditional legal protections. Therefore, SECONDO will implement the intelligent Big Data Collection and Processing Module (BDCPM) that uses specialised crawlers to acquire risk-related data either from internal organisation sources, e.g. network infrastructure or external sources such as social media and other internet-based sources.

There is a wide range of methods and approaches for conducting quantitative risk assessments. Quantitative tools rely on numbers to express the level of risk. Typically, quantitative risk assessments have more transparency, and the validity of the analysis can be more easily determined. Quantitative risk assessment relies on models and can range from simple to complex [9].

The below subsections provide an overview of Quantitative Risk Analysis methods/modules:

2.1.1 QRAS

Quantitative Risk Assessment System (QRAS) [10] [11] [12] is a PC-based software tool for conducting probabilistic risk assessments (PRA). The tool was initially developed in 1997 in order to provide NASA with a PRA tool responsive to the agency's specific needs in the area of its space mission risk assessment [13]. Risk models in QRAS consist of representations of risk scenarios in the form of event sequence diagrams and fault trees linked through event sequence diagrams (ESDs). These models are organized based on a structural or functional decomposition of the system, as well as a decomposition of the system's mission timeline into phases and subphases.

The software (QRAS application), which runs as a standalone application on Microsoft Windows platforms, has a set of graphical user interfaces, which allow the user to perform the modelling and analysis operations. Additionally, the algorithms used in QRAS are: Binary decision diagrams, Fault tree Binary Decision Diagrams (BDD) construction, Sequence BDD construction

- The Proportional Risk Assessment Technique (PRAT)
- The Decision Matrix Risk Assessment (DMRA)
- Quantitative Assessment of Domino Scenarios (QADS)
- The Weighted Risk Analysis (WRA)

SECONDO modules will implement the Risk Analysis Ontology and Harmonisation Module (RAOHM) that receives the outcomes of the existing risk analysis tools and harmonises them using a common vocabulary with a straightforward definition in order to be used by QRAM.

2.1.2 Game Theoretic Module (GTM)

Game theory is the typical theory for use for decision-making when two or more rational decision-makers (intelligent adversaries) are involved in cooperative or conflictive decision situations. Although risk analysis and game theory are very different methodologies, however, by linking them, we will significantly improve the quality of forecasts and risk assessments. As described in [14], the workflow of setting up a Game Theoretic mode is depicted in Figure 1. The detailed comparison of how game theory fits into and aids the classical risk management process has been described by [14].

In [15], the authors propose a game-theoretic model for the insider problem, which they call an "insider game". An insider game is built on a stochastic game, a game played in a non-deterministic state machine that can describe most computing systems. The model captures other vital properties, especially the system administrator's uncertainty about the system state due to the insider's hidden action. Equilibrium strategies are computed to predict the insider's actions and identify the best way to respond to them. A potential solution is to adopt a simpler but less general type of game (e.g., an extensive game) to model a specific insider problem. Another enhancement is to model an incentive mechanism that discourages a potential insider from launching an attack. This can be achieved by adjusting security policies or techniques that change the structure of an insider game.

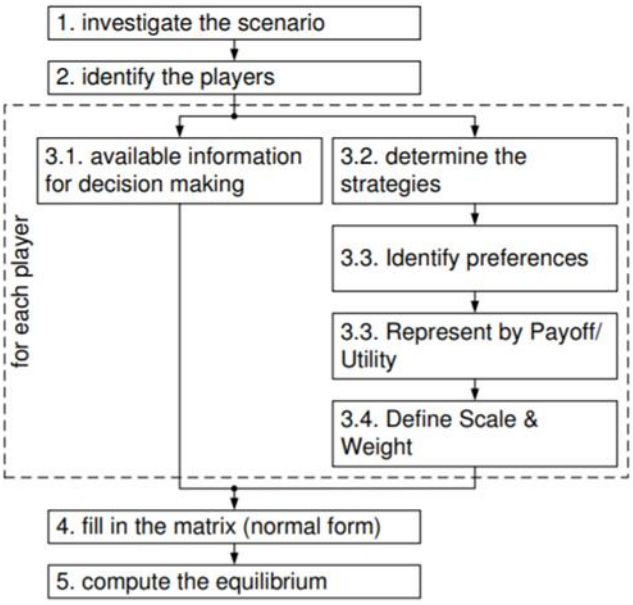

Figure 1 Workflow of setting up a Game Theoretic Model [14]

[16] provided a preliminary study on using game theory for determining the relationships between loss function tolerance and conditional risk. It provides a method for indicating how much a loss function can be modified in order to provide optimal approximation accuracy and precision. This is very useful for the users as determining the amount of tolerance they should have when modifying loss functions is difficult.

Another Game-Theoretical Model for Security Risk Management of Interdependent ICT and Electrical Infrastructures is presented in [17]. The authors model interactions between an attacker and a defender by using game theory. They derive the minimum defence resources required and the optimal strategy of the defender that minimizes the risk of the power system.

The risk score in Cyber Security Game [18] is calculated by using a mission impact model to compute the consequences of cyber incidents and combining that with the likelihood that attacks will succeed. The likelihood of attacks succeeding is computed by applying a threat model to a system topology model and defender model. Cyber Security Game takes into account the widespread interconnectedness of cyber systems, where defenders must defend all multi-step attack paths, and an attacker only needs one to succeed. It employs a game theoretic solution using a game formulation that identifies defence strategies to minimize the maximum cyber risk (MiniMax).

2.1.3 Continuous Risk Monitoring Module (CRMM)

Continuous reporting and monitoring of strategic risks is a dynamic process that requires organization-wide participation. Continuous monitoring of strategic risks moves the risk posture of systems to a level that allows tracking over time, often in real-time, to raise awareness of changing vulnerabilities and processes and provide for more effective decision-making regarding third party risk.

Organizations that support continuous monitoring a part of their holistic security, lifecycle-based risk management program that is designed in alignment with the organization's overall business objectives

would be expected to improve their ability to track and monitor critical third party vendor metrics, improve identification and proactive planning for remediation of issues as they arise and reducing the impact of cyber incidents [19].

Continuous Risk Monitoring and Assessment (CRMA) is a real-time integrated risk-assessment approach, aggregating data across different functional tasks in organisations to assess risk exposures and provide reasonable assurance on firms' risk assessments. CRMA includes processes that: a) Measure risk factors on a continuing basis, b) Integrate different risk scenarios into quantitative frameworks, and c) Provide inputs for audit planning [20].

2.1.4 Social Engineering Assessment Module (SEAM)

Social engineering is a method that seeks to exploit weaknesses in human nature and take advantage of the naivety of the average user. Although the techniques of social engineering have evolved over time, the success of such attacks still depends on modern preventive tools and the security systems in place, as well as the availability of trained and skilled personnel dealing with sensitive data in organizations [21]. On the other hand, Social Engineering is increasingly being used to help hackers bypass the initial IT security barriers. The SANS institute has published statistics about the trends of social engineering that reveal that social engineering techniques that bypass preventative measures are growing.

Many works in literature have been defined the term social engineering and tracking new techniques employed by its users, such as [22] [23] [24] [25]. In particular, the lack of social engineering awareness is a concern in the context of human cyber security risks. [21] highlights pitfalls and ongoing issues that organizations encounter in the process of developing human knowledge to protect from social engineering attacks. [26] investigates the level of susceptibility to social engineering amongst staff within a cooperating organisation. The results revealed that 23% of recipients were successfully snared by the attack, suggesting that many users lack a baseline level of security awareness that is useful to protect them online. [27] used an email-based approach in Sydney University, by sending emails to undergraduate computer science students improperly requesting usernames and passwords in the pretext of intrusion detection and subsequent system upgrade. 47% of students fell for this trick and provided their valid username and password details. Moreover, [28] used a physical approach, by posing to be an individual from an organisation's computer support department and asking employees for a range of information (e.g. usernames, passwords, etc.). The results finding from this study were alarming. The results show that around 80% of participants provided their username and almost 60% also provided their password.

2.1.5 Attack Graph

The attack graph model that was initially proposed by Phillips and Swiler [9] is used to construct a graph that represents all possible pathways an attacker may follow through the vulnerabilities exploitation. Topological Vulnerability Analysis (TVA) [29], Multihost, Multistage, Vulnerability Analysis (MULVAL) [30] used the monotonicity assumption to generate more compact attack graph. There are many other tools such as Skybox Security [31] and Red Seal Systems [32] etc. to generate attack graphs. These tools take the network devices configurations, and the vulnerabilities extracted by vulnerability scanners (e.g., Nessus [33], Nmap [34], or Retina [35]) as inputs. Additionally, [36] uses

the probabilistic method to calculate the network security metric. The authors of the paper select the next exploit (attack graph edge) randomly, with each edge have the same probability of being selected by an attacker. Anoop Singhal and Ximming Ou [37] also use probabilistic attack graph models and calculate quantitative metrics to score an enterprise network risk.

2.1.6 Bayesian Networks

A Bayesian Network is a graphical representation of a joint probability distribution over a set of statistical variables. The structure consists of a directed acyclic graph (DAG), made up of nodes that represent variables. Arrows between variables can represent direct causal dependencies based on process understanding, statistical, or other types of associations. These follow through different knowledge engineering processes, which can be executed either by experts. A conditional probability table (CPT) is used to describe the probability of each value of the child node, conditioned on every possible combination of values of its parent nodes. Bayesian Networks exploit the distributional simplifications of a network structure by calculating how probable events are, and how these probabilities change given subsequent observations or external interventions.

In [38], Bayesian networks are used for quantitative risk analysis in hospitals to improve patient's safety. Bayesian networks provide a framework for presenting causal relationships and enable probabilistic inference among a set of variables. Additionally, in [39], the authors have proposed a new methodology for combining expert elicitation and data by using the Bayesian network method for evaluating the risk. In risk assessment, models need to fit into an adaptive management context. Adaptive management involves learning from management actions and using that learning to improve the next stage of management. Bayesian networks can incorporate new information into the model as it becomes available and allow model parameters to be continually adapted and refined, enabling innovative responses to novel situations, and assisting in the learning process. Bayesian decision theory provides a solid foundation for assessing and thinking about actions under uncertainty. The Bayesian approach also provides aid for decision making as a tool for improving the qualitative analysis throughout numerical procedures [40] [41].

2.2 Optimal Investment in Cyber Security Blockchain

Cybersecurity has become a key element in the growth of almost any organisation. The potential impact of a cyber incident dictates taking seriously cyber security investment decisions so that besides making a financially feasible and optimal decision, the defence of the organisation is maximised while minimising the risk of catastrophic cyber-attacks. The objective of cybersecurity investment methodologies is to compute an optimal distribution of cybersecurity budget and one of the initial works studying this was performed by Gordon and Loeb [42].

In this section, we survey the most well-known and impactful articles in the field of cyber security investments and allocation of limited budget to protect an organisation, infrastructure and so on. The motivation behind designing and developing cyber security investment methodologies is in selecting optimal set of cybersecurity safeguards. These selections maximise the benefit of an organisation as they maximise the amount of risk they control. Undoubtedly, they are subject to some available budget, which can be seen as not only financial, for example time and resources.

One of the initial works studying the way to model investment in cyber security was published by Gordon and Loeb [42]. The authors consider the optimum level of investment given different levels of information security. The authors propose a model in which for any given vulnerability there are different levels of information security that can be implemented, where a higher level of information security will decrease the expected loss from that particular vulnerability. This is modelled as a function of the security level's responsiveness to an increasing vulnerability in reducing loss. In our model, here, we consider a single value for a vulnerability, and then for each control there are a number of levels of implementation, which represent the information security levels proposed by Gordon and Loeb. The main message of this work is that to maximise the expected benefit from information security investment i.e., an organisation should spend only a small fraction of the expected loss due to a security breach.

2.2.1 Cyber Security Investments

Gupta et al. [43] presented a Genetic Algorithm (GA) for matching cybersecurity technologies to vulnerabilities that they can patch. This matching problem exhibits the trade-off between maximising the number of vulnerabilities covered and minimising the costs for deploying the security technologies. Authors has reduced this problem to a set-covering problem and applied a GA for seeking the best security–vulnerability combination. The proposed heuristic algorithm was also faster than the Brute Force (BF) approach tested and its execution time found to increase almost linearly with the increase in the problem size determined by the number of cybersecurity technologies and vulnerabilities.

Rees et al. [44] were motivated by the challenging nature of quantification and measurement of: (i) threat metrics and (ii) efficacies of cybersecurity countermeasures. Their contribution is the development of a decision support system that in presence of uncertainties about threats rates, cybersecurity safeguards costs and asset losses, it calculates the system's risk. A characteristic of this system is that it empowers decision-makers to specify their own schema of data inputs so that they decide on the significance of the different values. It can also take as input an available budget and optimise decisions related to safeguards. Authors have assessed their system in a realistic use case from the manufacturing sector.

Likewise, Rakes et al. [45] were motivated by the difficulty in assessing and analysing the risk of threats and potentially catastrophic losses. They have extended previous mathematical models [46] to develop an integer programming model that optimises the selection of a subset of cybersecurity safeguards to mitigate certain threat level profiles. Authors assessed their model under expected and worst-case threat levels towards deriving trade-offs for optimal security planning between these two threat levels. They also demonstrated budget-dependent risk curves giving emphasis in showing how perturbed budget levels affect the aforesaid trade-offs. To demonstrate the analytical and computational feasibility of their approach on a set of larger problems, authors have used prototypical data available in the literature to demonstrate the analytical and computational feasibility of the approach on a set of larger problems.

In a similar vein, Viduto et al. [47] formulated a multi-objective optimisation problem to select cybersecurity safeguards in a cost-effective manner, taking into account both financial cost and

security risks. They proposed a novel risk assessment and optimisation model (RAOM) showing in a step-by-step process. As basis of RAOM, they used the NIST SP800-30 guidelines on performing risk assessments on which they made some modifications in impact and total risk calculation. The impact has been split into three types based on the Confidentiality-Integrity-Availability (CIA) model. Furthermore, they have developed a Multi-Objective Tabu Search (MOTS) algorithm to derive Pareto optimal points, which can satisfy security needs of the organisation in a cost-efficient manner.

Inspired by [45] and acknowledging the same challenge of assessing and analysing the risk of threats and potentially catastrophic losses, Sawik [48] applied two popular, in financial engineering (e.g. in portfolio management), measures of risk: value-at-risk and conditional value-at-risk. The author presents and assesses a model for selecting optimal cybersecurity safeguards based on threat likelihoods using prototypical data available in the literature. By incorporating analytical and computational feasibility analyses of large problems, the author offers a security risk planning tool that implements this model as a decision process.

Kauffman and Sougstad [49] were ones of the first to propose an application of a Value-at-Risk (VaR) method, and qualitative risk and reward trade-offs. Their VaR analysis is used in an optimisation model to provide actionable managerial decision support. They modelled the impact of IT contracts' duration and structure to risk exposure and provided scenarios where managers can reconfigure the timing of contracts to mitigate risk.

Inspired by [49], Lee et al. [50] applied the profit-at-risk and operational risk modelling approaches to propose a model that facilitates optimal customer information security investments by undertaking trade-off analysis between risk and return. They acknowledge that despite a lower probability of an information security incident, the associated risk may be significantly high because of high potential impact from compromised assets. The authors defined a minimum information security protection level that must be achieved for the investments in customer privacy protection to be effective.

Authors also considered, in their analysis, the impact of cost to implement and operate the protection. Finally, they argued that investing to achieve the maximum level of cybersecurity protection is often a non-optimal strategy due to ever-changing technologies and attack landscape which adversely affects the efficacy of chosen cybersecurity safeguards. Deane et al. [46] were motivated by the IT alignment within a supply chain and they proposed model to address this challenge. The key contribution of this model is in showing which part of the supply chain can have the most impact for the money spent in cybersecurity. They have applied the model to demonstrate the benefit of having organisations collaborating with each other to protect a supply chain.

Nagurney et al. [51] were motivated by the fact that complexities in the supply chains with multiple spatially dispersed entry points have led to vulnerabilities that cyber-attackers exploit to compromise these supply chains. Authors proposed a supply chain network game theoretic model consisting of retailers and demand markets. The retailers have to select their optimal product transactions and cybersecurity levels while the probability of a successful cyber-attack against a retailer depends on the cybersecurity levels of both themselves as well as the other retailers. On the other hand, consumers declare their demand price functions. The latter are a function of both the actual demand

and the network security level, which is equivalent to the average security of the supply chain network. Authors analyse nonlinear investment cost functions with budget limitations. They then show how cyber security investment cost functions vary according to consumers' preferences for the product, which, in turn, depends on both the demand and the security level.

Srinidhi et al. [52] propose an optimisation model to reason about the allocation of cyber security resources to assets that have inherent strength against cyber-attack and security-enhancing assets (i.e. security controls). They also investigate the role of cyber insurance in mitigating the effects of breach costs as well as the incentives that both managers and investors in spending upon cyber security products given that the first (i.e. managers) are more concerned with potential financial losses while the second (i.e. investors) are reluctant to spend more in strengthening the firm's security due to spreading their risks by investing in different firms. Lastly, Cavusoglu et al. [53] compare a decision-theoretic approach to game-theoretic approaches for investment in cyber security. Authors neither use real world data to undertake their risk assessment nor do they investigate the optimal selection of security controls.

Demetz and Bachlechner [54] provided a survey of models that have been proposed for the study of economic viability of tools for security policy and configuration. The authors identified a series of requirements that a security investment tool should contain, e.g. dealing with the regulatory and contractual requirements, such as GDPR. The main finding was that there is no single approach that is entirely suitable.

Another work on cyber security spending has been published by Smeraldi and Malacaria [55]. The authors identify the optimum manner in which investments can be made in a cyber security scenario given that the budget allocation problem is most fittingly represented as a multi-objective Knapsack problem. Their motivation is stemming from the scenario where an optimally set of cybersecurity safeguards, each having a cost and benefit, must be selected given a budget. Their proposed methods include optimisation algorithms that can deal with safeguards that exhibit non-linear relationships and a case where a safeguard can cover (i.e., protect) or leave a target uncovered given that safeguards cover several targets. They are also using standard dynamic programming to handle non-linear dependencies between the different safeguards.

Cremonini and Nizovtsev, in [56], have developed an analytical model of the attacker's behaviour by using cost-benefit analysis considering rewards and costs of achieving different actions. One issue that we factor into this work is that security comes at a cost that is greater than that of the price of implementing a policy. Wang et al. note that game-theoretic approaches to cyber security suffer from the fact that “the rationality of hackers is hard to be captured by a model, because they may be motivated by different value systems” [57]. While the authors do not argue on the rationality of the attacker, but the idea that imposing on them a similar set of values as a defender is not adequate. Previous work we have conducted in this area notes that the reward for the attacker is in line with the loss of the defender by the way of an affine transformation [58]. This was done to represent the loss of value that an attacker gets from the data that has been stolen, when compared to the value to the defender.

Fielder et al. [59] have proposed decision support methodologies for the optimal choice of cybersecurity safeguards within an investment budget. They have addressed cybersecurity investment decisions by proposing different approaches; a game-theoretic approach, a combinatorial optimisation approach and a mix of both called hybrid. To assess their methodologies, authors have created a realistic use case in which they use scores for vulnerabilities and attacks from the well-known CVE repository, but they have also considered the Critical Internet Security (CIS) controls as defending options of the organisation. For each safeguard (i.e. control), they defined a control-game which allows them to choose among different implementation levels of this particular safeguard trading safeguard efficacy with safeguard indirect cost (e.g. system performance). Solving these games produces game equilibria. In the second part of the papers, authors define a multi-objective Knapsack optimisation to derive optimal combination of safeguards game equilibria subject to a financial budget constraint. Interestingly, this paper confirms the advice of the UK government with regards to the optimal 5 cybersecurity controls that all SMEs must have in place.

Beyond previous works such as [59], [60], [58] and along the direction of optimal cybersecurity investments, Wang [61] investigated the cybersecurity investment balance between acquiring knowledge and expertise and deploying mitigation techniques. On the other hand, Chronopoulos et al. [62] have opted a real options approach to analyse the performance of optimal cybersecurity controls on organisations. In particular, the authors have analysed the effects of the cost of cyber-attacks and the time of arrival of cybersecurity controls on the organisation's optimal strategy. Similar to these papers, our work also considers the choice of the optimal strategy based on the efficacy of the control towards mitigating cyber risks.

Further, to achieve realistic cybersecurity investment models, researchers have investigated investment models with uncertainties such as uncertainty in vulnerability assessment [63] and uncertainty in risk assessment [60]. They have also derived Nash Defending Strategies under these uncertainties showing that cybersecurity investment models are capable of providing effective decision support even in presence of uncertainty.

Paul and Wang [64] investigated the optimal balance between prevention, and detection and containment safeguards under uncertainty. The authors have presented that adjusted prevention impacts social cost and optimal configuration of safeguards the most. They have identified gaps in existing cybersecurity frameworks' reliance on prevention and have proposed recommendations addressing the gaps. In the direction of cybersecurity resilience, [65] have modelled cybersecurity resilience based on the needed security controls to facilitate defined security functions. Considering affordable residual risk, budget, resiliency and usability constraints, the authors have proposed an optimal selection of critical security controls for optimal and resilient risk mitigation planning. Another recent and relevant, to SECONDO, paper is [66] where the authors have investigated the balance between investing in self-protection and cyber insurance. Their optimisation minimises expected risk and cyber insurance premium.

2.2.2 Blockchain in Cyber Insurance

Eling [67] brings some important issues cyber risk insurance and asks some important questions about its future. They state that as technology processes, it is likely that innovative business models will be

needed, giving the example of blockchain.

Henk and Bell [68] explains that block chain can bring many benefits and can aid greatly the insurance industry, however, this comes with many questions. Its structure can save claims costs and open new doors with marketing insurance, providing the ability to offer new products in a timely fashion. However, the insurance industry is far behind others when considering the implementation of new technologies. Henk and Bell state that it is likely this will carry on even with blockchain, as insures will likely want to wait to see blockchain function perfectly in other sectors.

Digrazia [69] informs that users and businesses alike should be aware of cyber threats because the Internet of Things has created a world that has resulted in us being reliant on data and being connected online. With this being the case, Digrazia expresses that if companies develop multifactor unique identifiers, that we could be better protected, and the blockchain could be key for this to occur.

Mohamed [70] explains that since e-commerce has become the core for any company to succeed, companies must protect their data as best as they can. With this comes the idea of e-insurance to protect these companies from risks. Insurtech is becoming more popular, with examples like cars and wearable monitoring technology being used to simplify insurance policies.

Feng et al. [71] proposes a risk management framework to protect blockchain providers from double spending attacks using a two-stage Stackelberg game. This game shows the interaction between block chain provider, cyber-insurer and users, which each have a role to play within risk management. They also examine equilibrium strategies of the three parties using backward induction and conducts simulations to evaluate performance. With this, is a need with this paper to then investigate the long running competition between provider and insurer.

Lepoint et al. [72] is another creation that can aid in protection. In this case the creation of BlockCIS to show how a system can implement a secure distributed infrastructure for assessing cyber risk within a company and shows how features such as selective disclosure of data can be added to what has been created. Here, Lepoint et al. want to further their work and test their creation in an operational environment to assess how accurate their model is in a real setting.

Vakilinia et al. [73] explores a new framework for insuring a cyber product using blockchain. To share the risk of insurance, crowdfunding is used via a sealed-bid auction process. They show the advantages of this framework and studied the implementation of a sealed-bid auction on blockchain as well as a method to reserve the bid values during the bidding process has been proposed. Finally, Vakilinia et al. makes an important note, that insurance companies are affected by cyber risk themselves.

2.3 Cyber Insurance and Smart Contracts

2.3.1 Cyber Insurance

Security incidents have become commonplace, with thousands occurring each year and some costing hundreds of millions of dollars. Consequently, the market for insuring against these losses has multiplied in the past decade. With the increasing data breaches, cybersecurity is quickly moving from being considered by business leaders as a purely technical issue to more considerable business risk.

Many companies are starting to consider cybersecurity as a significant business risk and, as a consequence, they are looking for methods to ensure the continuity of financial operations in case of cyberattacks.

Recently many academic works have been done trying to address individual problems of cyber insurance. The authors of [74] summarised different scientific achievements in cyber insurance through a survey on this topic. They have found that despite a slow start and many problematic issues, the cyber insurance market grows.

Cyber policies were initially designed to cover non-physical perils and damage to intangible assets (the cost of notifying individuals, IT forensics, credit monitoring, public relations and crisis management and communication are included). Recently, some cyber products are combined with other insurance policy types, such as technology errors and omissions liability insurance [75].

Moreover, a plethora of cyber-risk insurance policies exist in the marketplace. In addition to conducting very rigorous theoretical modelling of an insurance market, Marotta et al. [74] provided an overview of covered loss areas across 14 carriers. Majuca et al. [77] mainly described the evolution of insurance policies since the late 1990s, as well as provided an overview of covered losses from seven carriers, while Baer and Parkinson [78] review policies from six carriers. Furthermore, Woods et al. [79] examine 24 self-assessment questionnaires provided by insurance carriers.

The authors in [80] and [81] modelled network externalities and showed that a tipping phenomenon is possible, i.e. in a situation of low level of self-defence, if a certain fraction of the population decides to invest in self-defence mechanisms, it could trigger a massive cascade of adoption in security features, thereby strengthening the overall Internet security. Additionally, [82] shows that in a cyber insurance framework, cooperation amongst network users results in the latter making better self-defence investments than the case in which they would not cooperate. However, not all applications in cyberspace can be cooperative, and as a result, we consider the general case of non-cooperative application environments and to ensure optimal insurance-driven self-defence amongst users in such environments.

In 2016, the Cambridge Centre for Cyber Risk and Risk Management Solution had released the latest version of the Cyber Insurance Exposure Data Schema as well as a framework for Managing Cyber insurance Accumulation Risk in [83] and [84]. The first presents a schema that structures the data that should be captured in an insurer's cyber accumulation management system, while the second sets up a complete framework for assessment and understanding of cyber insurance accumulation risk management. Additionally, ENISA presents good practices and challenges during the early stages of the cyber insurance lifecycle [85], [86], [87].

[88] examined a sample of over 12,000 cyber events that include data breaches, security incidents, privacy violations, and phishing crimes. Specifically, the authors in [88] found that the cost of a typical cyber incident in their sample is less than $200k (about the same as the firm's annual IT security budget) and that this represents only 0.4% of their estimated annual revenues. Therefore, with increasing cyber-attacks and security breaches, insurance is more important than ever. Policy makers recognize the role of the cyber insurance market in enhancing cyber resilience.

[89] provided a series of policy recommendations aimed at enhancing the contribution of the cyber insurance market to managing this increasingly prevalent risk. The report examined the current state of the market, based on substantive input from the insurance companies etc. that are directly involved in its development, and the obstacles that are impeding the market from reaching its full potential.

Another useful study [90] compared the available scientific approaches to analyse of the cyber insurance market and summarise their findings with a common view. This approach helps us to find situations where authors disagree, and further research is required. Moreover, they defined various future directions of scientific and practical improvements in the area of cyber insurance.

[91] addresses the cyber insurance industry and its potential to act as both an actor to lessen the systemic cyber risk by improving enterprise cybersecurity practices, and as a potential source of systemic risk to the broader insurance market itself, were there to be large-scale covered damages to insured entities. First, this report offers insurance companies, cybersecurity experts, policymakers and other stakeholders a framework to identify and assess systemic cyber risks for the insurance market. Second, the report suggests policy recommendations for companies and governments to help address cyber risk for the insurance industry. These recommendations are intended to limit the exposure to systemic shocks with potentially catastrophic effects for the insurance market, including through the development of a government backstop and other measures. The report contributes to improving overall cyber resilience in the face of increasing cyber threats and global connectivity.

A global survey of scientific research in the cyber market [92] presented recently. Results indicate that, although the cyber market presents a significant opportunity for insurers, they need to be diligent about the significant risks and downside potential to writing this business, including limitations in historical data and uncertainties in accumulation risk. Moreover, it is essential to underwriting risks at the right price. This means that proper underwriting guidelines have to be in place, and pricing models need to be as robust and reliable as possible. While the cyber insurance market has been increasing recently, the insurance providers face several challenges, such as lack of standardised frameworks to rate "cyber," shortage of relevant data to calculate premiums etc. Unlike other types of insurance, cyber insurance requires creating a continuous feedback loop between customers and insurers [20].

Due to the continuously changing nature of cyber threats, a scenario-based modelling approach is crucial. Model validation and robust model risk management processes also are vital for a model to remain appropriate and sustainable in the face of constantly changing threats. Moreover, it is expected that regulators to require more robust validation of cyber modelling in the future. To cope with these increased requirements, internal validation teams may need training on this new and specialized area [92].

2.3.2 Smart Contracts

In 1996, cryptographer Nick Szabo wrote a paper [93] entitled "Smart Contracts: Building Blocks for Digital Markets" that he laid down the ground rules of Smart Contracts as one of the critical innovations of blockchain [94]. A blockchain is a shared ledger maintained by several nodes without a central authority. It typically achieves consensus using a distributed (Byzantine tolerant) cryptographic protocol. The blockchain concept first appeared in the Bitcoin cryptocurrency [95] as an immutable

record of transfers, maintained by all parties that hold and trade the currency.

However, past years have witnessed profound and disruptive implications of blockchains in a wide range of settings. It is now possible to specify business logic for transactions, ranging from recording who owns which asset to executing self-enforcing and complex functions (smart contracts). Smart contracts make it possible to distribute a business service among many parties, with potentially conflicting interests, to achieve a common goal. In [96], the authors introduce BlockCIS, a blockchain-based continuous monitoring and processing system for cyber insurance. BlockCIS aims to realise an automated, real-time, and perpetual feedback loop between the insurer, its customer, third parties and potential auditors. The most popular platforms of a smart contract are Bitcoin [97] and Ethereum [98]. As it was mentioned in [99] the taxonomy of smart contracts can be classified into five main categories: a) Financial, b) Notary, c) Game, d) Wallet and e) Library.

Smart contracts in Ethereum are computer programs written by a programming language called Solidity [100]. Any rules and functionalities can be written using compatible programming language and encoded as a smart contract to invoke whenever an action is required by users or other smart contracts. Different kinds of applications of financial instruments can be implemented such as cryptocurrency management) e.g. AlterDice [101]), crypto wallets (e.g., MyEtherWallet [102], MetaMask [103], and MyCrypto [104]), and autonomous governance applications [105], [106].

Smart contracts are self-enforcing pieces of software, which reside and run over a hosting blockchain. Using blockchain-based smart contracts for secure and transparent management to govern interactions (authentication, connection, and transaction) in Internet-enabled environments, mostly IoT (Internet of Things), is a niche area of research and practice. However, writing trustworthy and safe smart contracts can be tremendously challenging because of the complicated semantics of underlying domain-specific languages and its testability. The authors in [107] presented a comprehensive empirical evaluation of open sources automatic security analysis tools such as Oyente [108], Mythril [109], Security [110], and SmartCheck [111] for the security vulnerability detection of Ethereum smart contracts written in Solidity [100], [112], [113]. Moreover, different tools on ten real-world smart contracts from both vulnerability effectiveness and accuracy of valid detection viewpoints were tested. They concluded that IoT combined with smart contracts on blockchains are helpful in building more reliable and secure networks, and it would appear to hold great promise for future IoT security development. Moreover, the taxonomy of dependencies in smart contract vulnerabilities is a) Blockchain vulnerabilities, b) software security issues, c) Ethereum and Solidity vulnerabilities and d) security analysis tools which are addressed in [114]. The smart contracts' vulnerabilities are summarized in [115].

It should be noted that user privacy, contract confidentiality, precise execution and easy deployment are essential for the use of smart contracts. Hawk [116], a privacy-preserving smart contract was invented to protect user privacy and sensitive information of the contract without being leaked to the public. In [117], some plugins are designed to safeguard smart contracts from being the harm in deployment level. New consensus algorithms, like proof-of-stake and Byzantine fault tolerance algorithms, definitely help reduce energy consumption and improve efficiency. By using smart contracts, the traditional physical-based paper process and endorsement are turned into digital

formats that bring convenience to data management; the claim process is triggered by smart contracts automatically but also is accelerated, becoming decentralized with widely witnessed evidence. Additionally, privacy-preserving techniques are used in data storage and smart contract to protect clients' privacy.

3 General Insurance Challenges

Insurance is one of the vastest areas of world economy, and one of the most challenging of its field. Particularly, business insurance and all of its subcategories (i.e. aviation insurance, travel insurance, satellite insurance, marine insurance, shipping insurance) involve complex and thorough procedures, study and assessments, as well as the cooperation and coordination of the many parties included. Regarding companies and enterprises of any scale, the needs of smooth and efficient insurance applications are increasing, and of paramount importance. New technologies in insurance, a rapidly evolving field/industry, are addressing the various challenges that emerge, proposing novel solutions and improvements to the traditional insurance operations.

In business, insurance consists of a complex network of multiple parties interacting with each other constantly, exchanging data and performing transactions at high amounts. Such processes are both time and money consuming for all parties involved, and can entail various challenges and risks, such as various delays in data exchange and updates, or even complete lack of data, compliance being undermined, the occurrence of errors, duplication or fraud, the increasing of costs or the overall inefficiency of the processes. Also, often insurers only audit the security of a system and test the controls applied in defence after an actual incident and claim, when the procedure takes a lot of precious time and resources and of course, since the damage is already done, has no meaningful impact but serves only in evaluating the situation. [118]

Furthermore, due to the high numbers of players, transactions and intermediates between the ends, risk transfer to the insurance market is too complex of a procedure, often acting in an obstructive manner. This also adds to the overall time of the process as a whole, as the many stakeholders interact with each other at all times, exchanging large amounts of data as mentioned before. Due to the complexity of the system, should an issue occur, or the system infrastructure require an update, the procedure of checking or changing it would be extremely complex and time consuming. [76] [118] [150]

Credibility is also at stake, as the integrity, availability and accuracy of the data exchanged are not always ensured, at least to an acceptable degree. The many different types of stakeholders, such as the clients, insurers, brokers and so on, exchange multiple types of data (i.e. deck logs, ship routes, cargo information, customer information) of the utmost importance, that can be delayed, compromised, intercepted or altered due to either error or malevolent intentions, with grave consequences to the entire ecosystem of parties involved. Specifically, as much of the data is handled or inserted manually, by employees of the company or companies, their Credibility is also at stake, as the integrity, availability and accuracy of the data exchanged are not always ensured, at least to an acceptable degree. The many different types of stakeholders, such as the clients, insurers, brokers and so on, exchange multiple types of data (i.e. deck logs, ship routes, cargo information, customer information) of the utmost importance, that can be delayed, compromised, intercepted or altered due

to either error or malevolent intentions, with grave consequences to the entire ecosystem of parties involved. Specifically, as much of the data is handled or inserted manually, by employees of the company or companies, their accuracy can be questioned due to human error. As for the transactions between the parties involved, they are often evidently subjected to delays or riddled with errors, thus either damaging one or more parties or costing the participants time to fix the errors and evaluate the process. All of the above, as well as the participants' trust in the system and each other. This is reinforced by the lack of transparency in most of the procedures and agreements, or the lack of thoroughness in studying all aspects beforehand. It is often the case of insurance claims not being paid and cases being settled in court, because of disagreement of the parties on the courses of action chosen, lack of mutual trust and information being withheld. This can cause damage to the reputation of the participants, can take months or years to be settled and cause great financial damages to all parties in legal fees, potentially not deciding in favour of the wronged side in the end. [74] [76] [86] [119] [120] [121]

As per usual in every aspect of security, the human factor is the weakest link of the chain, rendered unreliable as a part of the ecosystem when it comes to the data and its processes, as well as many procedures of the insurance as a whole. Often when regarding one specific party’s interests, there is always the possibility of fraud, and tampering with the data or even withholding it, aiming to benefit the company that employs them. That is not to say of course that all data altered is due to malevolent intentions, as it is far more common for procedures to be susceptible to human error. Apart from the technical aspects of course, one must take into account the various legal procedures that may need to be followed through, e.g. a claim agreement or case resolution to be led in court. In that case, the outcome is dependent on the people involved, namely lawyers, attorneys, witnesses, juries and judges. [76] [86] [119] [121]

Last but definitely not least in the series of challenges is the fact that various new types of threats are emerging in the environment of enterprises, with a prominent example being that of the cyber threats concerning the system’s infrastructure. This of course involves various new challenges that have yet to be fully taken into account. Generally, most enterprises are not fully aware of the new types of threats. Thus, they have very limited view and knowledge of both the emerging risks as well as the countermeasures they can take to prevent or limit the possible impact, should they occur. As for the insurance companies, such knowledge is only now coming to the spotlight, with no existing historical data on these new types of threats as reference. Furthermore, in certain cases, the legal framework is not yet in alignment with new needs for adequate insurance of all assets of the companies, i.e. in the case of cyber threats, companies may not be abided by law to disclose their cyber information with the insurance company, making the following courses of action on all parties unclear. Another notable outcome of the emerging cyber threats can be identified in the insurance process itself, as the communication and exchange of data that may be confidentially passed from one party to another, may be subjected to cyber-attacks, such as Man in the Middle, and consequently be intercepted, tampered with or have access to it denied from the rightful owners. An overall issue as well is the lack of transparency in the various insurance procedures and decisions based on the transactions between the actors, i.e. the client and the insurer, as previously mentioned. This, in conjunction with the aforementioned issues, creates an environment that is not optimal for any of the parties involved.

[74] [76] [86] [119] [120] [121] [150]

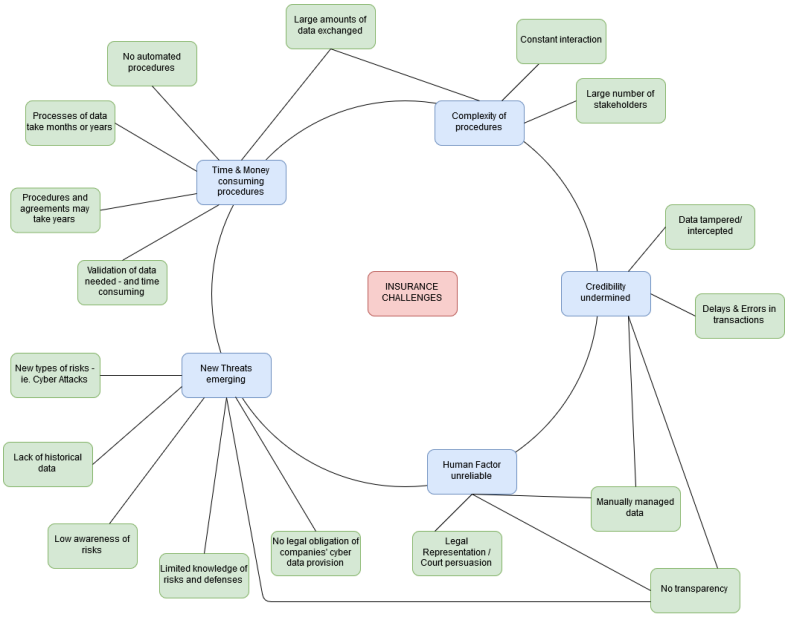

Figure 2 General Insurance Challenges

4 Cyber Security Incidents

Notable cases of cyber-attacks worldwide, with imminent effect to the insurance, have occurred in the previous years. Ever since the WannaCry attack, cyber-crime has become a prominent issue concerning both companies and cyber insurers. The cases vary both in the cyber risk at hand as well as the outcome concerning the insurance. One of the greatest cyber threats that befalls upon enterprises, especially in recent years, is that of ransomware, with extreme rise since 2016. For instance, the NotPetya ransomware that affected many enterprises in 2017 when, by a zero-day exploit. Many companies were severely impacted by the attack, which turned out to be originating from Russia and exploiting an accounting software from Ukraine. Therefore, the attack was considered an "act of war", due to the tense political situation in the area at the time, and insurance companies refused to cover for the damages, which amounted to millions of dollars. Thus, companies would cover the damages themselves, such as Mondelez that had to pay $100.000.000, Maersk with damages reaching up to $300.000.000 and Merck that had to pay $800.000.000 in damages. Another example would be the Marriott cyber-attack of the eponymous hotel firm, where up to half a billion guests' information had been compromised in 2018, going as far back as possibly 2014, causing not only major losses in the company's reputation and implementation of countermeasures, but also a great fine under the GDPR of up to $120.000.000 due to the leak of guests' personal data. Part of the reason for this and the lack of insurance coverage was that the risk was not known or taken into account, nor the new personal data regulation, as the firm purchased the Starwood hotel chain and all its infrastructure, including the guests' data and the ensuing risk, therefore the cyber insurance was not covering such issues and the company was unprepared for such a data breach. [124]

In the case of cyber-attacks on the city of Baltimore and the city of Atlanta, both in 2019, it is quite obvious how the company decides to handle the situation can define the outcome even more

decidedly than the cyber insurance would. More specifically, in both cases government computer systems were attacked by the ransomware RobinHood demanding approximately $300 per device. In both cases, ransom payment was denied. Though in Baltimore there was no cyber insurance, and the ransom amounted to about $76.000, the overall damages were about $5.300.000. However, in Atlanta's cyber-attack (SamSam virus) the system was insured, the overall ransom summing up to $51.000 and the insurance company suggesting that the ransom payment was the best option, in the end it was denied costing the city around $8.500.000 in recovery expenses. Another recent example is that of the Sodinokibi cyber-attack (ongoing), a ransomware that spreads via phishing emails and has very low detection rates, that has spread throughout Asia and lately Europe, affecting smaller companies such as dental firms, and compromising their data. Here it is obvious that each insurance company reacts differently to such attacks, some having taken the risk into account, some providing support and some none whatsoever. For instance, CTS had many of its clients affected by the ransomware but refused to pay the $700.000 ransom. Lastly, enormous data breaches such as Capital One's ensued great damages of up to $500.000.000, of which the insurance company can cover up to $400 million following a $10 million deductible, but the reputation damage remains. Lastly, in the National Bank of Blacksburg. Everest National Insurance Co. case the agreement of the coverage was settled in court, in a legal procedure that lasted for over a year. After refusing to pay out the full amount, the insurance company covered both cyber-attacks that occurred within the year for up to only $50.000, while the damages reached up to $2.400.000 for the Bank, on the grounds that such an attack was not covered by their insurance. [122] [123] [143] [144]

One of the greatest data breaches of the decade is that of Target, where the company had a cyber insurance policy of up to $100.000.000 coverage with $10.000.000 deductible, however the breach costs, including fees and compensations, reached as of 2016 around $300.000.000 with major impact to the company's reputation and profit. Similar cases include the Equifax data breach, in 2017, which compromised 143.000.000 clients' personal data, and though the insurance company covered for the damage as settled upon, it was inadequate as the loss was greater. Home Depot's data breach in 2014 causes $105.000.000 in damage which was fully covered by the various underwriters the company was insured under. Finally, Lloyd's have presented a cyber-attack scenario on various major ports of Asia's east coast. According to the scenario, a cyber-attack of a virus spreading from cargo ships to networks on Asia - Pacific major ports would have an economic impact of up to $110 billion, with only 8% of the losses being insured. [142] [123] [145] [125] [126]

5 Use Cases

5.1 Introduction

This chapter presents the high-level requirements analysis through four (4) use cases, their scenarios, and the modules that interact within the SECONDO platform. The following four use cases are described:

1. Use Case 1 - Human susceptibility to cybersecurity breaches in IoT-enabled smart home.
2. Use Case 2 - Optimal Patching of Airport Cyber Infrastructures.

3. Use Case 3 - Cyber insurance for an Innovative SME.

4. Use Case 4 – Cyber Risk Transfer in Maritime Industry.

These use cases are described in a way that expresses the use of the SECONDO platform and comprises all the functionalities that will be integrated in the final project output.

5.2 Methodology

Requirements in broad terms need to be discovered, documented and maintained (i.e. changing if necessary, keeping track of change and potential impact on the design, and validating the requirements once the process is over). These activities are referred to as Requirements Elicitation, Requirements Analysis, Requirements Specification, Requirements Validation and Requirements Management according to Robertson & Robertson in [3].

Requirements Elicitation is where the requirements process starts. It ensures a common understanding of the problem that the system aims to solve. The requirements elicitation involves collecting information about all involved stakeholders, including end users. The information that is sought is about what users are currently working with, why it is inadequate, what their vision of an improved system is, and why. To elicit requirements, there are many different techniques that can be used (interviews, surveys, brainstorming, etc.), sometimes in combination. For the purposes of SECONDO, we are primarily going to be using use cases.

Requirements Analysis The main objectives of Requirements Analysis are: To detect and resolve conflicts between contradicting requirements and more importantly to provide detailed requirements: an initial set of high-level requirements describing the functional characteristics of the overall system is followed by a step by step approach of decomposing it into more detailed functional and non-functional requirements. Several levels of requirements are developed, providing sufficient granularity so that they can be allocated to individual subsystems and components in the next step of system design. Similarly, in the case of SECONDO, a prioritization is going to take place prior to embarking on system design. Consulting with the stakeholders and end users, more important technical requirements are going to surface in order to provide a highly relevant system design.

Requirements Specification is the formal documentation of the requirements extracted from requirements analysis. Requirements must be specific, so that they leave no room for ambiguity or misinterpretation. The specification document in the case of SECONDO the D2.1 has to be maintained over the life of the project.

Requirements Validation ensures that requirements are complete, consistent, unambiguous, accurate, necessary and feasible. Validation is different to verification, which merely determines whether the end system meets the requirements. Validation is a critical step that intends to identify requirement shortfalls as early as possible, when correcting them is less costly. Once requirements are validated through a review process, the requirements spec becomes the basis for all development and testing activities that follow.

Requirements Management fundamentally addresses traceability and change management of the

requirements themselves by any means appropriate depending on the complexity of the system.

5.3 Terminology

5.3.1 Participating modules

- Quantitative Risk Analysis Metamodel (QRAM): utilises advanced security metrics to quantitatively estimate the exposed cyber risks, taking into account important parameters not currently considered by existing risk analysis tools.

- Risk Analysis Ontology and Harmonisation Module (RAOHM): receives the outcomes of the existing risk analysis tools and harmonises them using a common vocabulary with straightforward definition in order to be used by QRAM.

- Social Engineering Assessment Module (SEAM): interacts with users to devise their behaviour using penetration testing approaches and it provides specific numeric results on risky actions.

- Big Data Collection and Processing Module (BDCPM): uses specialised crawlers to acquire risk-related data either from internal organisation sources, e.g. network infrastructure or external sources such as social media and other internet-based sources.

- Game Theoretic Module (GTM): models all possible attacking scenarios and defensive strategies and then uses game-theoretic techniques to derive optimal defending strategies in the form of Nash Equilibria (NE).

- Cyber Security Investment Module (CSIM): will be responsible to infer optimal investment plans. CSIM will be empowered by GTM.

- Econometrics Module (ECM): provides estimates of all kinds of costs of potential attacks and it takes into account costs, (i.e. purchase, installation, execution, etc.), of each possible security control using a set of existing econometric models.

- Continuous Risk Monitoring Module (CRMM): assesses on a continuous basis the performance of the implemented risk-reducing cyber security controls allowing the adaptation of the cyber insurance contract to the changing IT environment and the evolving cyber threat landscape.

- Cyber Insurance Coverage and Premiums Module (CICPM): computes cyber insurance premium curves and coverage as a function of the organisation's security level. These can be used by clients to determine desirable levels of cyber security investment prior to any cyber insurance contract agreement.

5.4 Use Case 1 – Human susceptibility to cybersecurity breaches in IoT-enabled smart home

5.4.1 Use Case Motivation

IoT has created a surge in technologies that aids user's daily lives. With this comes the many cyber and cyber-physical risks that can affect each user. Since this is the case, the need for cyber insurance has

grown to protect users in many different locations, such as within smart homes or smart offices. Since IoT is still undefined in many of its attributes, there is a need to understand how IoT affects risk management and how it would vary from other sectors. It is not only devices that introduce risks but the users themselves. Users have become reliant on data and as a result of this the risks brought by IoT need to be carefully considered and their impacts known. Furthermore, when designing a smart device cybersecurity policy, we must consider new attacks due to the continuous evolve of IoT. User awareness and familiarity can affect cyber risk, with many factors being part of the risk identification and assessment. With this comes the susceptibility that users have depending on many different attributes, and the impact on one's domestic life, as presented in [129]. Smart Home users use devices every day for many different reasons, which is why building a cyber risk assessment model for the individual will be important. As stated by Radanliev et al. [130], there is a lack of development models that assess IoT's impact, and this causes issues when putting a price to IoT cyber risk, with there being a lack of ability to price these in the same way that others do. As a result, any cyber insurance framework for smart homes will need to be empowered by appropriate cyber risk management models. One of the stages of developing these models, in SECONDO, would be to perform a quantitative risk analysis using QRAM. SECONDO will use this module to identify the types and value of risks related to the user. Cyber insurance and smart contracts are also important within this scenario, as building models with IoT cyber insurance in mind will build to the best quality coverage for users. With this being said, SECONDO's cyber insurance ontology has the potential to aid the creation of a good framework that considers IoT as well as general cyber risk.

5.4.2 Scenario

We assume there is an IoT-enabled smart home that serves a household of four; one couple, a teenager, and an elder person. All these users possess a number of personal devices, but they also have access to some shared devices. Every device of the household is considered to be part of the IoT infrastructure that we want to insure. An insurance premium will be added to the house insurance of the household covering cyber risks subject to a number of clauses provided by the underwriter. To achieve the computation of such premium, in this SECONDO use case, we take the following steps. We have assumed, in this use case, that SECONDO is used by the cyber insurer to derive optimal values of premium and coverage.

First, RAOHM will communicate with the current tools that the cyber insurer uses for conducting cyber risk assessment within the smart home. Then RAOHM harmonises these results using a common vocabulary and then send them to QRAM that quantitatively estimate the cyber risks within the smart home. A number of IoT threats will be used for the computation of risk values. Further, SEAM will be used to assess cyber risks inflicted from adversarial behaviour against users and the risk the latter introduce to the entire household. The same module also assesses all different 4 members of the household in terms of their cybersecurity level (i.e. vulnerability), which is used when undertaking the risk assessment by QRAM. In the next step, ECM estimates all costs that relate to the attacks that could occur in the smart home and the controls that may need to be implemented. CSIM is deployed, based on modelling and computations of GTM, to derive optimal ways to control the overall cyber risk in this use case. In parallel, CRMM is monitoring the use of cybersecurity controls and assessing their performance in terms of maintaining the expected level of risk. Any deviation can trigger the adaption

of the changing IoT risk scope. Finally, CICPM is used to derive an optimal contract for the household, i.e. premium and coverage.

5.5 Use Case 2 – Optimal Patching of Airport Cyber Infrastructures

5.5.1 Motivation

After a request from one of the biggest airports in the world, a European-based SME has been ordered to conduct a detailed Cyber Risk Assessment, Vulnerability Discovery and Vulnerability confirmation on the airport's IT infrastructure for Audit Purposes. The entire network topology was scanned, all vulnerabilities were disclosed, and their existence was confirmed. An instance of UBI' tool, called OLISTIC, was used and all acquired data from the assessment was fed to the Risk Assessment component of it. OLISTIC identified multiple critical infrastructure points (i.e. vulnerabilities) that their probability of getting compromised were highlighted and indicated as Very High. Should these vulnerabilities be exploited the entire airport infrastructure is under the control of the adversaries. This is due to the access privileges and the network topology that exhibits a high degree of interconnections between the discovered vulnerabilities and critical airport assets. One of the devices that is of critical importance and was identified as very likely to be exploited is a network router, which was running an old version of firmware. Even worse, the same router exists in every subnet of the airport making the final number of vulnerable routers to be larger than a hundred.

5.5.2 Scenario

The list with all possible exploitable devices was given to the airport management team and they were suggested to patch all of them. Their main challenge for patching these was not monetary resources themselves (e.g. purchased software) but the time of senior personnel, which must be spent to other critical operations. The situation was worsened due to the current size of the personnel working on the security and network department. This is comprised by 5 experienced individuals.

In this use case, we will demonstrate that with the use of SECONDO platform, this patching could have been attainable as GTM and CSIM modules can be used to propose optimal ways to undertake this complex and demanding task. Before the execution of these modules, UBI will take advantage of the functionalities offered by the QRAM, RAOHM, BDCPM and ECM modules. All these will extend the current risk assessment functionalities of their OLISTIC tool as follows.

5.6 Use Case 3 – Cyber insurance for Innovative SME

5.6.1 Motivation

CloudAndTech is an innovative SME that offers Business-to-Business (B2B) solutions for big data analytics and intelligent algorithms as well as professional services related to cloud computing and development. CloudAndTech has no physical infrastructure. All the development and production environments are hosted in the Google Cloud. It also uses tools for development such as Gitlab. Apart of the virtual infrastructure for building and deploying its solutions, it uses professional accounts for hosting the company's accounts, such as email and storage, collaboration environment for the team to work remotely.

Having no physical infrastructure (e.g., data centres) offers flexibility and does not require special

security measures to be taken, apart of course for securing access to its virtual infrastructure. CloudAndTech implements VPN and secure access-authentication procedures to ensure that access to its resources is not granted to unauthorised people. The cost for running all its business in the Google cloud and the other services is in the below 8,000 EUR per month. Losing the online infrastructure will cause the pause of its business. The customers will not be affected as their applications are running on their premises, but development, testing and some support tasks will not be able to continue. Code, customer related information and files will be lost (backups are being taken of course from time to time).

5.6.2 Scenario

CloudAndTech rents a physical office in Spain where it has been recently reported that a group of cyber criminals has launched a social engineering attack targeting innovative SMEs. CloudAndTech has decided to undertake Cybersecurity Risk Assessment using the SECONDO platform. Its result will indicate how CloudAndTech must spend their limited cybersecurity budget and whether they must outsource some of the risk to a cyber insurer. It is usually the case that SMEs prefer to treat cybersecurity investments and cyber insurance in a careless way so that they can prevent charges.

In this use case, we will use the SECONDO platform to demonstrate to CloudAndTech managers the importance of investing in cyber controls as well as outsourcing risk subject to the results of the risk assessment. More specifically QRAM, RAOHM, BDCPM and ECM will be used to undertake the desired risk assessment of their online and any other infrastructures while GTM and CSIM will compute optimal ways to invest a pre-defined cybersecurity budget. Last, CICPM will be used to derive optimal premiums and coverage so that CloudAndTech senior management team can decide how much of the risk to outsource. The latter will also take into account that CloudAndTech has filed a couple of patents related to intelligent algorithms that it has designed and developed. The risk of leaking the code or design of these applications is not considered to be high but in any case, the patent should ensure the ownership of the idea and the implementation.

5.7 Use Case 4 - Cyber Risk Transfer in Maritime Industry

5.7.1 Motivation

The maritime sector is a vital component in the trade and transportation field. In the recent past, physical attacks, i.e. piracy, were the common threats. After the adoption of electronic systems such as sonar and cyber systems in both onshore and onboard environments, new cyber and cyber-physical vulnerabilities emerged. However, quite often cyber losses are excluded from insurance coverage as the impact of a potential cyber-attack can be considered too uncertain to be included in policy terms. Until recently, indirect damages caused by cyber-attacks or errors (for example, damage to the ship due to navigation system malfunctioning after being hacked) would not be covered by non-cyber insurance policies, due to a specific cyber-attack exclusion clause ([10/11/2003] also known as Cl.380). According to the clause, insurers would not cover for damages caused by a cyber-attack if they would include bodily harm, business interruption or property damage. Other exceptions may include terrorism-related attacks and the NMA2914 electronic data exclusion. These cause the so-called "cyber insurance gap". However, due to the drastic increase in incidents of cyber-attacks, there has been much discussion on expanding the coverage of such attacks. Furthermore, as more and more

cyber occurrences emerge, with varying impacts to the affected company, it is becoming evident that the aftermath of a cyber-attack is not always contained to the digital assets.

Since cyber insurance is still a developing field, many aspects of the procedures and policies are still being determined. One such aspect is the distinction between affirmative and silent or non-affirmative cyber. In affirmative cyber risk, it is clearly and positively stated in the insurance Property and Casualty (P&C) policy that the insurer shall cover the costs in the case of data breach and/or network failure or attack, whatever the impact may be (physical, digital, human etc.). On the other hand, silent or non-affirmative cyber refers to unknown or unquantified exposures that are caused by cyber-attacks or incidents and may affect traditional property. Non-affirmative cyber risk occurs when insurance policies are 'silent' on the matter, in that they don't explicitly either include or exclude it. As per European Insurance and Occupational Pensions Authority (EIOPA): "Non-affirmative cyber risk refers to instances where cyber exposure is neither explicitly included nor excluded within an insurance policy. The latter type of cyber risk is also referred to as "silent" cyber risk. Two main implications can result from non-affirmative cyber exposures: first, some insurers may pay claims for unforeseen cyber losses when they have not charged a premium for this risk in certain circumstances, and second, depending on the cyber incident, it can trigger accumulation of losses within other policies." [146]

As there are still unknown areas in cyber risk and relative technologies are rapidly evolving, new challenges emerge. It is becoming increasingly evident that more and more cybersecurity incidents occur in the marine field, but extremely few are being reported and officially made public. Usually, only major cyber-attacks are being made public and well-documented, such as the Maersk attack in 2017. Thus, the underreporting on such cases, the limited knowledge on the matter and the existing incidents and the lack of historical background on marine cyber-attacks creates a "false sense of security" to marine companies, where the chances and impact of a potential cyber-attack are heavily underestimated. More often than not, marine companies will purchase the most basic insurance, either disregarding completely the cyber risks or assuming they are included in the insurer's coverage. In the case of the latter, the company and the insurer are usually not on the same page - therefore presenting the second category of challenges. Marine companies and insurance companies may have miscommunication issues with the terms that are being used, as well as the mutual understanding of the produced agreements. The insured-insurer communication needs to be absolutely clear and the terms of agreement, the traditional and cyber coverage, as well as the possible exceptions to be clarified upon agreement. [147] [148] [149] Coverage capacity, risk estimation and appropriate solutions are difficult for insurers to manage at this point, leading to a margin of the so called silent (unintended) cyber coverage. If, for instance, a cyber-attack was to cause damage to a company's physical equipment, network failure (downtime) or generally lead to business interruption and the subsequent losses, it is possible an insurer would not have the capacity for coverage. In some cases, the insurance company may add a premium charge for adding non-affirmative cyber coverage, but given the rapidly evolving technologies, varying impacts and increasing number of cyber incidents in marine SME, this will not be a viable solution indefinitely. According to the CSO Alliance, more than 1,000 ships have successfully been hacked in the last five years. Standard Hull and Machinery Insurance does not cover: i) Breach Responses Costs and System Restoration; ii) Income Loss and Expenses from a Breach; iii) Third Party Costs and Regulatory Fines; iv) Advice from specialists during

an incident. In this use case we aim to present a risk transfer situation where a shipping company transfers its risk to a third party. By third party we mean the Insurance. In our use case this will happen by purchasing an insurance policy. The shipping company purchases an insurance policy by the insurer and gets insured against financial risks. If the threat is high priority when internal mitigation techniques are not able to reduce the risk, then the decision to transfer the risk by insuring against loss is the only solution. The risk transfer contains the following steps: i) Risk assessment; ii) Risks management and iii) Insurance exposure estimation, coverage and premium calculation. The following table demonstrates the differences between the standard Hull and Machinery Insurance and the standard Cyber Insurance.

Table 2 Differences between the Standard Hull and Machinery Insurance and the standard Cyber Insurance

Cyber Covers	Standard Hull and machinery Insurance	Standard Cyber Insurance	Ideal Cyber Insurance
Breach Response Costs and System Restoration	NO	YES	YES
Physical Damage to the Vessel	Infrequently	NO	YES
Income Loss and Expenses from a Breach	NO	YES	YES
Third Party Costs and Regulatory Fines	NO	YES	YES
Access to Pre=Breach Education	NO	Occasionally	YES
Access to Specialists During a Breach	NO	YES	YES

5.7.2 Hull Cyber Cover

We assume that a shipping company wants to insure its ship. The ship has the following assets: i) Communication Systems; ii) Navigation Systems; iii) Sensors; iv) Propulsion System; v) Crew; vi) Operators; vii) Cargo Management; viii) Mooring System and ix) data. These assets are vulnerable in both cyber and physical attacks. The above assets can endanger the company's financial situation, reputation, property, crew's life and file the environment. The insurance processes are as follows:

Phase 1. Risk Assessment

Risk assessment is conducted through external tools, its results are input to the RAOHM. Then, RAOHM harmonizes the produced results utilizing a common vocabulary and then sends them to QRAM, the module that makes a quantitative estimation of the cyber risk values in the shipping company's infrastructure, using various known cyber and cyber-physical maritime threats. SEAM will be used to assess malevolent cyber risks inflicted by adversaries attacking the ship, systems,

equipment and people working in the shipping company, as well as the behaviour and response of the shipping company's employees in regard to cybersecurity. Finally, the shipping company will provide their proposed insurance coverage based on their assets, risks and turnover to the Asset Pricing.

Phase 2. Risk management

Through GTM all possible attack scenarios and the optimal courses of action and defence are calculated. Then, ECM estimates of all kinds of costs of potential attacks by taking into account demands (i.e. purchase, installation, execution, etc.) of each possible security control using a set of existing econometric models. Furthermore, CRMM assesses on a continuous basis the implemented risk-reducing cyber security controls' performance, thus allowing the adaptation of the cyber insurance contract to the always changing IT environment and evolving cyber threat landscape. These submodules constitute the CSIM, which will then update the blockchain. The results of these submodules are subsequently processed to provide optimal investments' recommendations.

Phase 3. Cyber insurance exposure estimation, coverage and premium calculation.

Finally, CICPM collects the results of the aforementioned modules, in order to produce the computed insurance premium and coverages. After the premium is set by the insurer, the broker communicates with the shipping company in order to analyse the contract and explain the premium. Should the shipping company accept the contact, premium and coverage then all three main players (the shipping company, the broker and the insurer) strike a final deal, transferred on the blockchain as a smart contract. This smart contract is equipped with the full coverage as its account balance and with a list of actions that represent the claim actions. During the smart contract lifetime, the CICPM continuously communicate with the CSIM in order to check for possible violation of the smart contract.

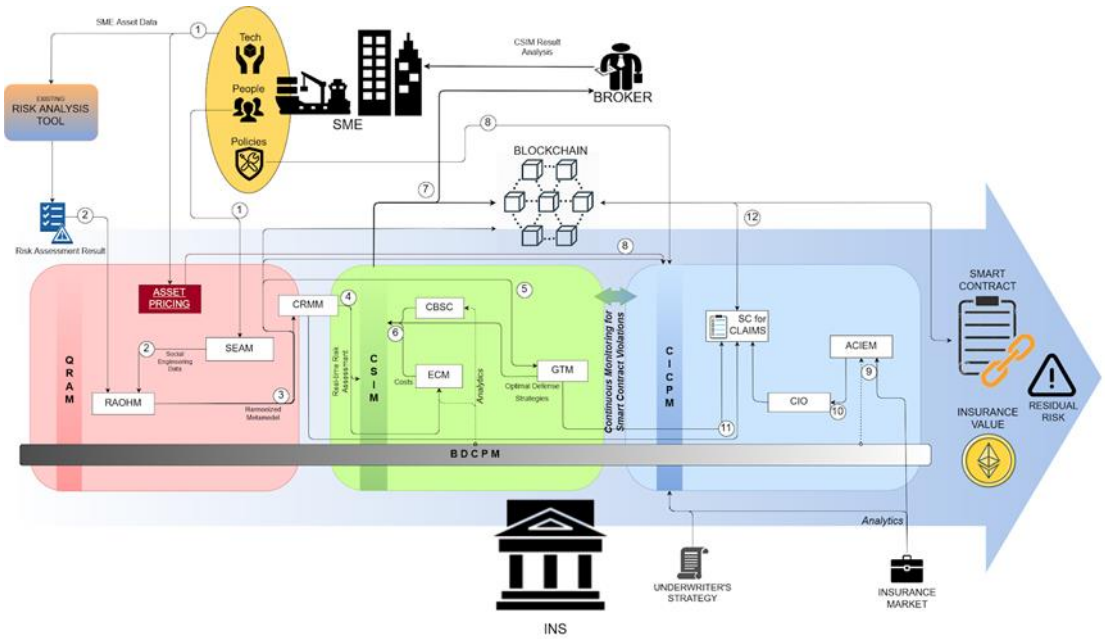

Figure 3 - Risk Transfer with SECONDO

We assume that the shipping company XYZ has a smart contract with its insurer the INS. The broker is

the BROKER company. After consulting the Insurance company, the XYZ requests the coverage for claims, as estimated, requesting a risk transfer on their part. The shipping company must provide the necessary information on its compliance with various guidelines as prerequisites for the Insurance company. Such prerequisites are compliance with BIMCO cyber security guidelines, the International Maritime Organization's Resolution on IT and OT systems, best practices and risk management, as well as the ISO cyber security standards compliance. On the other hand, the Insurance company performs a secondary risk assessment, utilizing RAOHM, thus estimating the potential damage, premium and coverage required through ECM. Cyber system failure can have serious impact on marine safety, as networks, mails, data and administration can affect the smooth operations, company's finances and of course reputation, but OT related risks (i.e. SCADA or engine cyber control) can additionally impact physical property, cargo and machinery, the environment and people's safety. Now that the insurers have a clearer view of the risks and costs, they utilize GTM to calculate the optimal courses of action and incident response strategies. After all of the above, the Insurance company and the Shipping company settle on the strategies, the premium as well as the coverage as requested by the XYZ, all of which are agreed upon the produced smart contract.

Hull Cyber Cover contains the following coverages:

- INS will pay on behalf of XYZ for any Breach Response Costs.
- INS will pay the XYZ for any Restoration Costs.
- INS will pay the XYZ for any Income Loss and Extra Expense.
- INS will cover for any physical property (hull and machinery) loss or damage caused by any electronic/cyber related error or attack.
- INS will reimburse the Insured for any Cyber Extortion/Ransomware Payments and any Cyber Extortion/Ransomware Expenses.
- XYZ will execute INS advice.
- INS will pay on behalf of the XYZ any Damages and Defense Costs.
- INS will pay on behalf of the XYZ any Regulatory Penalties and Regulatory Investigation Costs.
- INS will not cover for any Income loss and expenses incurred during the time retention.
- The XYZ has to cooperate with INS in all investigations.
- The XYZ has to maintain or update its defense against its risks.

Hull Cyber Cover Benefits:

- Error or attack detection leads to immediate action/control application, minimizing the impact.
- Automation of procedures minimizes the chances of errors.

- Automated repayments.
- Strict authorization and access control since in the private ledger only authorized entities have access.
- Privacy-preserving smart contacts to hide insured's personal and sensitive data.
- Real-time system monitoring for smart contract violation.
- Data immutability, since the stored data in the private ledger cannot be modified or deleted.
- Trust, since cryptography ensures trust between parties and a transaction that has been validated via user credentials cannot be repudiated.
- System transparency ensures the insurer's and insured's mutual trust on the system.
- Automation of procedures ensures fast incident response and other necessary processes.
- Various modules (GTM, ECM) ensure the optimal course of action selected.
- INS will provide various mitigation services to the SME, such as employee training in risk awareness and handling, tools and software to minimize cyber risk, as well as other resources within and out of the company, providing information on existing risks.
- INS will provide support services to the SME, handling calls from customers in the event of an incident, specialized and triaged support to the company itself in handling the incident, as well as the cyber insurance coverage and costs.

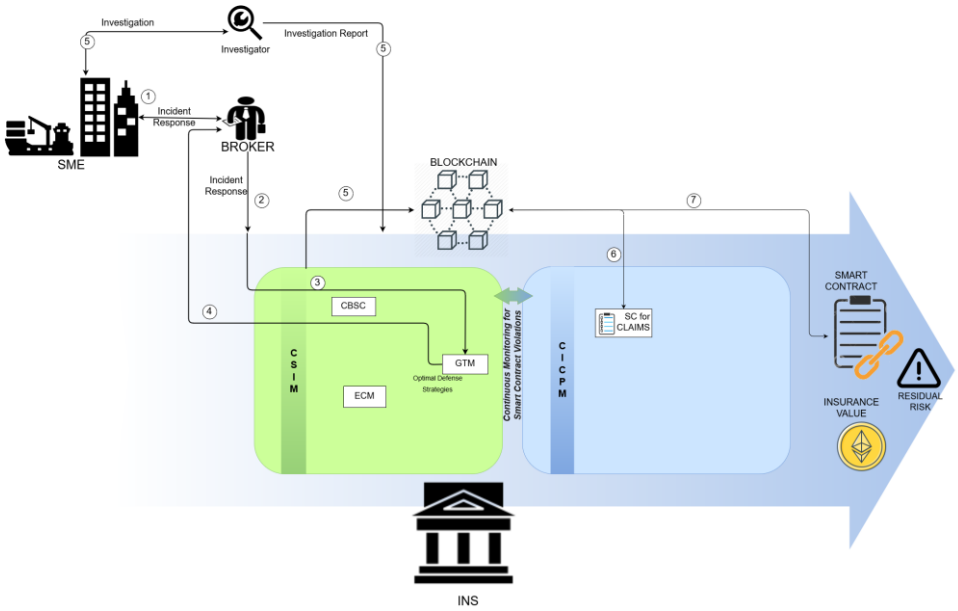

Figure 4 - Incident Response with SECONDO

After the successful operation of the shipping company, the XYZ is under a cyber-attack. XYZ is a victim of the ransomware called CryptoMarine. Its payload encrypted the files of all hard disks and the back-

up files. Also, it encrypts the sensors which collect data on tank levels, nitrogen oxide concentration, temperature and other on-board parameters. These values cannot be displayed anymore. Furthermore, the navigation system, communications are down, not permitting the ship to successfully communicate with the onshore operators. This attack affects the XYZ at a total, since its property, crew and reputation are jeopardized. XYZ's share price is going 10% down. Customers who transfer their products with the XYZ worry about their safety. The attackers demand ransom in cryptocurrency to unlock the encrypted devices.

5.7.3 Attack Timeline

A XYZ employee identifies the incident (the ransomware infection) and, according to the XYZ's disaster recovery policy the responsible officers as well as the INS are contacted immediately. Upon realising the ongoing attack, the business continuity plan is set in motion. The Emergency Response Team is called to action, which then assembles:

- A Disaster Recovery Team (DRT), responsible for key services restoration and business continuity achieved as quickly as possible
- A Business Recovery Team (BRT), consisting of senior members of the main departments and management team, who are responsible for the company's operation recovering as quickly as possible
- A Media Team, to be in contact with the media if needed and ready to answer basic incident questions (i.e. what happened, how it happened, how is it being handled)

Concurrently, the INS is contacted. The INS is closely cooperating with the company to ensure that immediate incident response actions are taken, and the recovery plan is applied. While efforts focused on the company's data backup are being made, the insurer enlists Forensic Experts to assist the company with the cyber defence efforts while, concurrently, Personal Relations (PR) assistance is also deployed in order to manage the communication with the company's clients that have either been affected by the attack (i.e. cannot track their cargo, cannot access the system etc.) or possibly feel insecure about their goods being handled in the future due to the system failure. PR experts will be assisting the company with handling their customers' concerns but also the Media Team with possible media pressure inquiring about the attack, in case the events are leaked outside the company.

According to the insurance company's approach, paying the ransomware is the last resort. Other alternatives must be attempted first. First and foremost, the existing recovery plan must be applied. Existing back-up countermeasures, adopted by XYZ prior to the incident, are implemented to relieve some of the issues. It is necessary that there is a complete system back-up, predating the infection so as to avoid restoring an infected instance. However, the back-up should also be quite recent, to avoid the loss of critical business operations data. Secure back-up should be kept offline in a separate and secure location and be taken frequently. If not done properly, this countermeasure may not be adequate in the case of such an attack. Furthermore, there is always the chance that the ransomware is not new. In this case, it is possible and probable that solutions against this particular ransomware (such as existing keys, decryptors, ransomware removal tools) have already been found and are available. The competent bodies responsible for addressing the matter and ensuring immediate business recovery are entrusted to attempt every measure possible in order to combat the

ransomware quickly and rescue the company's data and systems. DRT and BRT, in cooperation with INS experts, need to work on the systems restoration and attempt to disinfect it from the ransomware before the ransom time expires, while alternate measures are taken to attempt business continuity in the shortest period of time possible. If all back-up and recovery efforts are fruitless, and no known countermeasures against the specific ransomware seem to work within the margin of time given before payment, then and only then the insurance company advises XYZ to pay the ransom.

Since there is an incident active, the INS initiates investigation immediately. The results of the investigation are input to their smart contract. Smart Contract automatically initiates its process to assess the damage and decide which actions will be executed. If XYZ was totally compliant with its insurance policy, with no violation of the Smart Contract as evident by the CRMM output, then the coverages will be followed. The loss is estimated, and the results of the investigations reveal that the ransomware was an attachment on an email received from a ship agent in a port. Unfortunately, the updated firewalls and antivirus could not identify it and prevent it from infecting the marine company's system. The XYZ and the INS acted immediately and through the blockchain all the actions executed automatically.

6 Technical Requirements Specification

This section contains the technical requirements for each of the modules of the system based on the use cases and user stories, as well as the proposed system architecture.

6.1 Quantitative Risk Analysis Metamodel (QRAM)

Table 3 QRAM Requirements

#	Functional Requirements	Rational / Comments
F1.1	The mechanism should run existing risk analysis tools.	This is a basic requirement of the QRAM functionality. The output of the risk analysis tools will be given as input to RAOHM.
F1.2	The mechanism should define the parameters for the risk analysis tools.	In order to execute the risk analysis tools, the QRAM will take into account important parameters not currently considered by existing risk analysis tools.
F1.3	The mechanism should interact with the Risk Analysis Ontology and Harmonisation Module (RAOHM).	RAOHM is one of the modules of QRAM.
F1.4	The mechanism should interact with the Social Engineering Assessment Module (SEAM).	SEAM is one of the modules of QRAM.
F1.5	The mechanism should interact with the Big	The BDCPM will provide input data to the modules

	Data Collection and Processing Module (BDCPM).	of QRAM.
F1.6	The mechanism should support different risk analysis tools.	In order to be able to address different use-cases.
F1.7	The mechanism should receive input from the External Sources (input from organizations)	This is a basic functional input for QRAM.
#	**Non-Functional Requirements**	**Rational / Comments**
NF1.1	The mechanism should provide a clear interface to define new parameters and security metrics.	In order to enhance the usability of the platform.
NF1.2	The mechanism should be easily extensible to new parameters and security metrics.	In order to enhance the extensibility of the platform.
NF1.3	The mechanism should be extensible to new risk analysis tools.	In order to enhance the extensibility of the platform.
NF1.4	The mechanism should provide ease of use to operators of the platform.	In order to enhance the usability of the platform.
NF1.5	The input from organizations must be protected while being transferred.	In order to address security concerns.

6.2 Risk Analysis Ontology and Harmonisation Module (RAOHM)

Table 4 RAOHM Requirements

#	Functional Requirements	Rational / Comments
F2.1	The mechanism should receive the output of existing risk analysis tools, as input.	This is a basic functional input for RAOHM.

F2.2	The mechanism should receive the output of the Social Engineering Assessment Module (SEAM), as input.	This is a basic functional input for RAOHM.
F2.3	The mechanism should harmonize the outcome of the risk analysis tool using a common vocabulary.	This is the basic functionality of RAOHM.
F2.4	The mechanism should recognize new emerging threats.	In order to extend existing security ontology methodologies by factors that so far have not been considered in the literature.
F2.5	The mechanism should recognize the assets and the countermeasures that can lower the probability of incident occurrence.	This factor will extend existing security ontology methodologies.
F2.6	The mechanism should recognize potential loss regarding both intangible and tangible assets.	This factor will extend existing security ontology methodologies.
F2.7	The mechanism should recognize the speed of threat propagation.	This factor will extend existing security ontology methodologies.
F2.8	The mechanism should provide the risk analysis ontology representation in semantic web languages.	In order to increase the applications of the produced security ontology.
F2.9	The mechanism should perform asset identification.	In order to identify the critical assets; an output that will be used for the risk analysis.
F2.10	The mechanism should be able to implement the CORAS Language method.	The CORAS method will be used for the representation of the ontology in semantic web languages.
#	**Non-Functional Requirements**	**Rational / Comments**
NF2.1	The mechanism should provide a clear interface and procedures for defining the risk analysis ontology.	In order to enhance the usability of the platform.

NF2.2	Any sensitive information regarding the clients should be protected.	In order to address security concerns regarding organization's data.
NF2.3	The mechanism should be easily extensible to different use cases.	In order to enhance the extensibility of the platform.
NF2.4	The mechanism should provide fast communication between the modules as well as reliable data transfer.	In order to enhance the performance of the platform.
NF2.5	The interface for the CORAS Language method should ensure usability.	The modules of the platform should be user-friendly.

6.3 Social Engineering Assessment Module (SEAM)

Table 5 SEAM Requirements

#	Functional Requirements	Rational / Comments
F3.1	The mechanism should have access on users' devices.	Penetration tests will perform on users' devices.
F3.2	The mechanism should be able to monitor multiple devices, simultaneously.	SEAM should collect data from different types of resources.
F3.3	The mechanism should be able to monitor the users' actions, in real time.	The continuous input from the users' devises is necessary for the functionality of SEAM.
F3.4	The mechanism should store the data of the users' actions.	In order to provide numeric results on users' actions constantly updated.
F3.5	The mechanism should provide numeric results on users' risky actions.	In order to quantify the organization defense ability against the social engineering attacks.
F3.6	The mechanism should use the outcome of the security training and awareness programs.	SEAM will receive input data from external resources.
F3.7	The mechanism should interact with the	SEAM will provide input data to RAOHM.

	Risk Analysis Ontology and Harmonization (RAOHM) module.	
F3.8	The mechanism should be able to perform penetration testing methods.	In order to model the users' behavior.
#	**Non-Functional Requirements**	**Rational / Comments**
NF3.1	The mechanism should provide secure connection with the users' devices.	In order to address security concerns in regard to users' personal data.
NF3.2	The communication protocol between the mechanism and the users' devices must be lightweight.	In order to enhance the performance of the platform.
NF3.3	The mechanism should be easily extensible to a new type of users' devices.	In order to enhance the extensibility of the platform.
NF3.4	The mechanism should easily be adaptable to new use cases.	In order to enhance the adaptability of the platform.
NF3.5	The mechanism should ensure that all users' personal information will not be linked to a physical person.	In order to address security concerns.
NF3.6	The mechanism should be able to address network failures.	In order to enhance the resilience of the platform.

6.4 Cyber Security Investment Module (CSIM)

Table 6 CSIM Requirements

#	Functional Requirements	Rational / Comments
F4.1	The mechanism should interact with the Game Theoretic Module (GTM).	GTM is one of the modules of CSIM.
F4.2	The mechanism should interact with the	ECM is one of the modules of CSIM.

	Econometrics Module (ECM).	
F4.3	The mechanism should interact with the Big Data Collection and Processing Module (BDCPM).	BDCPM will provide input data to the modules of CSIM.
F4.4	The mechanism should be able to receive as input the results of the Big Data Collection and Processing Module (BDCPM).	The BDCPM provides analytics on Internet sources regarding state-of-the-art security solutions as well as their cost.
F4.5	The mechanism should determine the optimal cyber security investment.	The basic output of CSIM.
#	**Non-Functional Requirements**	**Rational / Comments**
NF4.1	The mechanism should provide a clear interface regarding the input data from the supporting modules.	In order to enhance the usability of the platform.
NF4.2	The mechanism should ensure secure data transfer between the supporting modules.	In order to address security concerns.
NF4.3	The mechanism should use a lightweight protocol which will coordinate the supporting modules.	In order to enhance the performance of the platform.

6.5 Game Theoretic Module (GTM)

Table 7 GTM Requirements

#	Functional Requirements	Rational / Comments
F5.1	The mechanism should interact with Quantitative Risk Analysis Metamodel (QRAM).	In order to receive input data (Asset pricing).
F5.2	The mechanism should interact with Continuous Risk Monitoring Module (CRMM).	In order to receive input data (the output of CRMM).

F5.3	The mechanism should interact with the Cyber Insurance Coverage and Premiums Module (CICPM).	In order to provide input data to CICPM (optimal defending strategies and cost).
F5.4	The mechanism should construct high-level attack scenarios.	The mechanism will employ Attack Graphs.
F5.5	The mechanism should define the defensive strategies for each high-level attack scenario.	In order to formulate a one-shot Game for a given defending-attacking scenarios.
F5.6	The mechanism should be able to simulate defending-attacking scenarios.	In order to validate hypothetical attacks.
F5.7	The mechanism should formulate each defending-attacking scenario as one-shot game (Game Theory).	In order to compute the optimal defensive strategies.
F5.8	The mechanism should compute the optimal defensive strategies in the form of Nash Equilibrium.	The Nash Equilibria of a given one-shot Game correspond to the optimal strategies.
F5.9	The mechanism should estimate the cost of attacking and the cost of defending, for each attacking scenario.	In order to provide input data to CICPM.
F5.10	The mechanism should specify the optimal allocation of a cyber security budget.	In order to provide input data to CICPM.
#	**Non-Functional Requirements**	**Rational / Comments**
NF5.1	The mechanism should provide secure storage for the data related to the defending-attacking scenarios.	In order to address security concerns regarding organization's sensitive data.
NF5.2	The mechanism should compute fast the Nash equilibrium of a given one-shot game (defending-attacking scenarios).	In order to enhance the performance of the platform.

NF5.3	The mechanism should use a clear interface where the platform operators will define the defending-attacking strategies and scenarios.	In order to enhance the usability of the platform.
NF5.4	The mechanism should be extendable to different use cases.	In order to enhance the adaptability of the platform.
NF5.5	The mechanism should compute fast the optimal budget allocation.	In order to enhance the performance of the platform.

6.6 Econometrics Module (ECM)

Table 8 ECM Requirements

#	Functional Requirements	Rational / Comments
F6.1	The mechanism should estimate a price value for each organization's tangible asset.	By applying existing asset-pricing methods.
F6.2	The mechanism should perform cross section analysis of organizations using the ORBIS database.	In order to estimate lower and upper values for each organization's intangible assets.
F6.3	The mechanism should estimate the cost of all potential attacks as well as the cost of all possible security controls.	In order to provide input data to the method that will compute the optimal cybersecurity budget allocation.
F6.4	The mechanism should be able to run a variety of econometric models.	In order to support the basic functionality of asset-pricing.
F6.5	The mechanism should interact with the continuous risk monitoring module (CRMM).	In order to receive input data regarding the risk assessment.
F6.6	The mechanism should interact with the Game Theoretic Module (GTM).	In order to take input data regarding the Nash Equilibrium defending strategies.
F6.7	The mechanism should formulate the budget allocation problem as an instance of the multi-objective multiple-choice Knapsack problem.	In order to estimate the optimal organization's cybersecurity budget based on the cost of the Nash equilibrium strategies.

#	Non-Functional Requirements	Rational / Comments
NF6.1	The mechanism should secure storage of any sensitive information regarding the participating organizations.	In order to address security concerns.
NF6.2	The mechanism should be able to run fast the econometric models.	In order to enhance the performance of the platform.
NF6.3	The mechanism should be able to compute fast an approximate solution to multiple-choice knapsack problem.	In order to enhance the performance of the platform.
NF6.4	The data transfer between the connected modules should be reliable and secure.	In order to enhance the performance of the platform.

6.7 Continuous Risk Monitoring Module (CRMM)

Table 9 CRMM Requirements

#	Functional Requirements	Rational / Comments
F7.1	The mechanism should periodically evaluate the risk-reducing cyber security controls.	Adaptation of the cyber insurance contract to the evolving cyber threat landscape.
F7.2	The mechanism should perform risk identification.	This is part of the risk management process.
F7.3	The mechanism should perform risk treatment.	This is a part of the risk management process.
F7.4	The mechanism should periodically perform risk monitoring.	This is a part of the risk management process.
F7.5	The mechanism should estimate cyber insurance risk coverage.	One of the main goals of CRMM.
F7.6	The mechanism should serve as mediator between the insurance company and the	In order to receive input data.

	client who has requested the insurance.	
F7.7	The mechanism should measure how the residual risk of an organization affects personal data under GDPR.	This is an important issue regarding the personal data inside EU zone.
F7.8	The mechanism should simulate the risk propagation on the organization assets.	In order to determine the organizations' total risk level.
F7.9	The mechanism should determine the impact of a potential risk controls failure.	In order to determine the organizations' total risk level.
F7.10	The mechanism should periodically record risk values using the blockchain of SECONDO platform.	In order to store the data with a secure and immutable method.
F7.11	The mechanism should interact with the Big Data Collection and Processing Module (BDCPM).	In order to receive input data.
F7.12	The mechanism should interact with the Risk Analysis Ontology and Harmonisation Module (RAOHM).	In order to receive input data.
#	**Non-Functional Requirements**	**Rational / Comments**
NF7.1	The mechanism should be easily adapted to dynamic evolving cyber threats environment.	In order to enhance the adaptability of the platform.
NF7.2	The mechanism should ensure secure data transfer between the system components.	In order to enhance the performance of the platform.
NF7.3	The mechanism should perform risk monitoring fast.	In order to enhance the performance of the platform.
NF7.4	The mechanism should be extendable to different use cases.	In order to enhance the extensibility of the platform.

NF7.5	The mechanism should be able to support secure data-transfer and storage.	In order to address secure concerns regarding sensitive data.
NF7.6	The mechanism should have a fast connection with the blockchain module.	In order to enhance the performance of the platform.

6.8 Cyber Insurance Coverage and Premiums Module (CICPM)

Table 10 CICPM Requirements

#	Functional Requirements	Rational / Comments
F8.1	The mechanism should interact with the Cyber Security Investment Module (CSIM).	In order to receive input data.
F8.2	The mechanism should interact with the Continuous Risk Monitoring Module (CRMM).	In order to receive input data; the conditions that violate cyber insurance contract agreements.
F8.3	The mechanism should take the selected defending policies, as input.	Necessary input for the CICPM mechanism.
F8.4	The mechanism should interact with the Big Data Collection and Processing Module (BDCPM).	In order to receive input data (analytics on cyber insurance environment and market).
F8.5	The mechanism should provide insurance exposure assessment and estimates insurance coverage and premiums.	The basic output of CICPM.
F8.6	The mechanism should provide insurance exposure assessment and estimates insurance coverage and premiums.	The basic output of CICPM.
F8.7	The mechanism should be able to deploy a private Ethereum blockchain.	The smart contracts will be implemented by this blockchain protocol.

F8.8	The mechanism should use non-deterministic smart contracts.	1) The smart contracts are privacy-preserving; They are able to protect sensitive client information. 2) The non-deterministic approach is suitable for the communication of the smart contract with all SECONDO components.
#	**Non-Functional Requirements**	**Rational / Comments**
NF8.1	The mechanism should ensure secure storage of any sensitive client information.	In order to address security concerns.
NF8.2	The mechanism should be easily extensible to new use cases.	In order to enhance the extensibility of the platform.
NF8.3	The mechanism should ensure the accuracy of the data exchanged.	In order to enhance the performance of the platform.
NF8.4	The mechanism should use a lightweight protocol which will coordinate the data transfer with the supporting modules.	In order to enhance the performance of the platform.
NF8.5	The mechanism should have a clear interface in order to ensure easy of use by the clients.	In order to enhance the usability of the platform.
NF8.6	The mechanism should compute fast the premium curves and coverages.	In order to enhance the performance of the platform.

6.9 Big Data Collection and Processing Module (BDCPM)

Table 11 BDCPM Requirements

#	Functional Requirements	Rational / Comments
F9.1	The mechanism should store the list of	Basic functional requirement for the crawler.

	sources that will be crawled.	
F9.2	The mechanism should be crawling each source from the list of sources, on a predefined time interval.	Continuous crawling. The crawler should pull updates from the web sources, multiple times per day.
F9.3	The mechanism should be able to interact with the three modules, namely the QRAM, CSIM and CICPM.	The BDCPM should provide input data to other modules.
#	**Non-Functional Requirements**	**Rational / Comments**
NF9.1	The mechanism should provide a high crawling bandwidth.	In order to enhance the performance of the platform.
NF9.2	The mechanism should be easy to operate and be maintained.	In order to enhance the usability of the platform.
NF9.3	The mechanism should be able to minimize the cost of the crawling operation.	High performance with minimum number of servers used.
NF9.4	The crawler should be able to handle network crashes.	The mechanism should be fault-tolerance.
NF9.5	The crawler should be able to interact with different web server configurations.	In order to enhance the adaptability of the platform.

7 Reference Platform Architecture

This chapter aims at giving more details about the main concepts and the components, to serve as a guide for the development of the project. SECONDO Architecture is driven by three high-level concepts/pillars (see in Figure 5 the yellow boxes): a) Enhanced Risk Assessment with security metrics and data analytics; b) Optimal Security Investment empowered by blockchain technologies to support cyber security and risk management; c) Cyber Insurance Policies Estimation supported by smart contracts. Each concept is represented by a component and the corresponding sub-modules namely: a) Quantitative Risk Analysis Metamodel (QRAM); b) Cyber Security Investment Module (CSIM); and c) Cyber Insurance Coverage and Premiums Module (CICPM) respectively. A high-level overview of the SECONDO architecture including the interactions among the components is depicted in Figure 5, while

Table 12 summarizes all the interconnections between components. The following subsections describe the main components/sub-components of the SECONDO architecture. For the purpose of SECONDO project, a platform will be created which will be designed to support the project purpose to assist organizations of any size and type to perform dynamically, continuously and near-real-time cyber-physical security risk assessment in compliance to the ISO/IEC 27001 standard and multiple other standards in order to narrow the gap between theoretical understanding and practice. All components of the SECONDO architecture will be described in sections bellow.

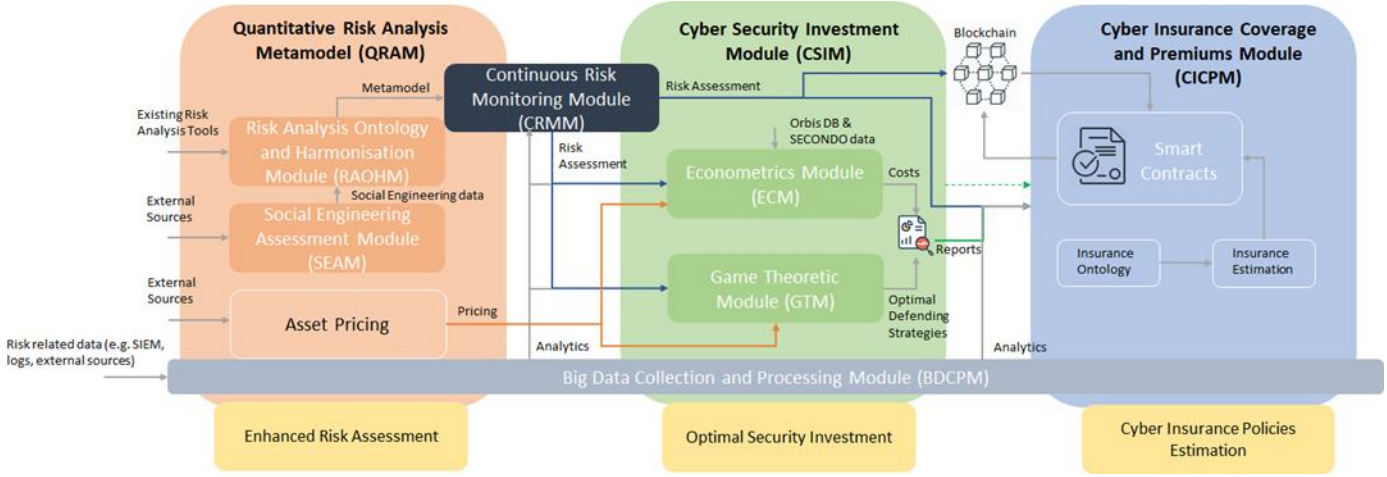

Figure 5 SECONDO High Level Architecture

Table 12 Inputs and outputs between SECONDO components and modules

Component	Module		Expected type of inputs / outputs	From / to	Defined in
Quantitative Risk Analysis Metamodel (QRAM)	Risk Analysis Ontology and Harmonisation Module (RAOHM)	Inputs	Existing Risk Analysis Tools	Open source risk analysis tools	WP3
			Social Engineering data.	SEAM	WP3

		Outputs	**Metamodel**	**CRMM**	**WP3, WP4**
	Social Engineering Assessment Module (SEAM)	**Inputs**	**Existing penetration testing tools**	**External Sources**	**WP3**
		Outputs	**Social Engineering data**	**RAOHM**	**WP3**
Continuous Risk Monitoring Module (CRMM)	**-**	**Inputs**	**Metamodel**	**RAOHM**	**WP3, WP4**
			Analytics	**BDCPM**	**WP3, WP4**
		Outputs	**Risk Assessment**	**ECM, GTM, CICPM, Blockchain**	**WP4, WP5**
Cyber Security Investment Module (CSIM)	**Econometrics Module (ECM)**	**Inputs**	**Risk Assessment**	**CRMM**	**WP4**
			Pricing	**External sources (QRAM)**	**WP4**
			Orbis DB, SECONDO data	**External sources**	**WP4**

			Analytics	**BDCPM**	**WP3, WP4**
		Outputs	**Costs**	**CICPM**	**WP4**
	Game Theoretic Module (GTM)	**Inputs**	**Risk Assessment**	**CRMM**	**WP4**
			Pricing	**External sources, QRAM**	**WP4**
			Analytics	**BDCPM**	**WP3, WP4**
		Outputs	**Optimal Defending Strategies**	**CICPM**	**WP4, WP5**
Cyber Insurance Coverage and Premiums Module (CICPM)	**-**	**Inputs**	**Reports**	**CSIM**	**WP4, WP5**
			Analytics	**BDCPM**	**WP3, WP5**
			Risk information	**Blockchain**	**WP4, WP5**
		Outputs	**Insurance Estimation**	**Blockchain**	**WP4, WP5**

Big Data Collection and Processing Module (BDCPM)	**-**	**Inputs**	**Risk related data (e.g. SIEM, logs, external sources)**	**External sources**	**WP3**
		Outputs	**Analytics**	**CRMM, CSIM, CICPM,**	**WP3, WP4, WP5**

7.1 Quantitative Risk Analysis Metamodel (QRAM)

Quantitative Risk Analysis Metamodel (QRAM) component will utilise advanced security metrics to quantitatively estimate the exposed cyber risks, taking into account important parameters not currently considered by existing risk analysis tools such as social engineering and already process information. More precisely, the QRAM component is a combination of the following subcomponents:

- Social Engineering Assessment Module (SEAM)
- Risk Analysis Ontology and Harmonization (RAOHM)

The purpose of QRAM component is to combine and analyse all the different collected data from the subcomponents and provide one unified data model. The QRAM component will identify all possible vulnerabilities of the assets, considering also social engineering, all possible threats that may exploit a resource in order to assist in the impact calculation and identification of mitigation controls. More specifically, this component is the first part of the risk analysis that identifies valuable digital assets and their vulnerabilities and reveals threats that may take advantage of those vulnerabilities. Then, it estimates the possible damage and expected losses resulting from the identified risks, in a well-defined unified and harmonized model and taxonomy analysis ontology. The main advantage of using a Quantitative approach is that it provides the ability to calculate any given not quantitative data like human behaviour, relate it with many other important aspects which are in scope and just by adding strict mathematical policies and rules you can quantify the non-quantitative data into numbers or other statistically oriented data. The main disadvantage of such model is the tolerance that is needed to be provided in errors. The reason for this is that mathematical models are strict and (ex. Human Behaviour) cannot always be defined as it should and sometimes the output should be included in quantitative fields that it does not fully belong. We do this to all collected data of a quantitative model, which means that we already know that some data will be ignored or misplaced on purpose. To implement the desired functionalities the QRAM, the following modules will be implemented:

7.1.1 Social Engineering Assessment Module (SEAM)

The Social Engineering Assessment Module (SEAM) interacts with users to devise their behaviour using penetration testing approaches and provides specific numeric results on risky actions (i.e. percentage of users that open suspect files or execute Trojans, etc.). In more technical detail, the readiness of the

employees of any organization against social engineering attacks will be evaluated. This module will include planning, targeting, means and evaluation of replicating such type of attacks. The planning phase will be the decisive part of which technological methods and axes will be used, such us email social engineering, client-side attacks like web browsing to a web page or even physical phone calls. The second part is targeting, which requires to find the target audience for our specific purpose. The third part is the means, which is a guessing of the correct attack for the correct target using also the most efficient tools (ex. Maltego, Social Media, etc.). Finally, all the collected data will be evaluated and provide the Social Engineering data output that feed directly to the RAOHM module.

Table 13 Input/output SEAM

INPUT: External Sources (input from organizations)
OUTPUT: Social Engineering data

7.1.2 Risk Analysis Ontology and Harmonisation Module (RAOHM)

In this module all concepts of SECONDO (e.g. risk, thread, attack type, behaviour, exploitation and impact) have to be formally represented. The output of existing risk analysis tool and the Social Engineering Assessment Module (SEAM) will be given as input to RAOHM, which then harmonizes them using a common vocabulary that will be developed for the specific purpose during the project's development lifecycle with straightforward definition in order to be used by CRMM. RAOHM will combine the seminal work on security ontologies proposed in literature and go beyond that, by additionally recognizing: a) current and emerging threats; b) which newly identified assets and countermeasures can lower the probability of incident occurrence; c) the potential loss regarding both intangible and tangible assets; and d) the speed of propagation of cascading compromises. These will be provided by developing entities, relationships, and diagrams between threats, vulnerabilities, security mechanisms, assets and risks. RAOHM will develop an efficient mechanism to identify the critical assets and use them for the risk analysis. The risk analysis ontology will expect to address the issue of sharing operational risk management information across the organization thus promoting the collaboration between business areas regarding the common as well as the horizontal operational risks. The ontology will aid the operational risk management group in gathering heterogeneous information from all business areas and communicating it effectively to the enterprise management in order to support the decision-making process the organization governance strategy regarding risks. Additionally, part of this mode is also the representation of the ontology in semantic web languages achieved using the CORAS Language method. The CORAS language is a graphical modelling language for communication, documentation and analysis of security threat and risk scenarios in security risk analyses. The language is an integral part of the CORAS method, which is based on the use of structured brainstorming. In these brainstorming sessions, the CORAS language is applied for making models of threat scenarios and risks on the fly. (see more information in section 6.3), which will enable the computation and inference over information residing in heterogeneous risk management applications of the organization, leading to the emergence of operational risk knowledge that could not have been realized by the individual applications and ways of introducing cyber insurance coverage complementary to the residual risk reduction.

Table 14 Input/output RAOHM

INPUT: Existing Risk Analysis Tools, Social Engineering data **OUTPUT**: Harmonized Metamodel

7.2 Big Data Collection and Processing Module (BDCPM)

The Big Data Collection and Processing Module (BDCPM) uses specialized crawlers to acquire risk-related data either from internal organization sources, e.g. network infrastructure or external sources such as social media and other internet-based sources. This module is a vertical one and interacts with all the three high-level components. This means that we will implement a central database that will acquire different types of data which will be defined as this project progresses. Intelligent Big Data analytics enables experts to build a predictive model that can issue an alert as soon as it sees an entry point for a cybersecurity attack. Analytics-based solutions enable organizations to predict and gear up for possible events in their processes. ELK Stack and Apache Spark will be used as the bases of this module. The collected data will be processed and give us statistical output which leads to higher and more efficient performance for the modules due to the existence of evaluation. Another use of the aforementioned module is to produce analytics and improve organization's defence and security as a whole. The data that will be collected and the different data sources will also be defined throughout the progress of the project. These data will again be processed and provide possible attack vectors, as well as any indication of advanced persistent threat (APT) of on organization.

Table 15 Input/output BDCPM

INPUT:	Internal & External sources (Risk related data). QRAM, CSIM, CICPM modules, user input/ logs/ files, data acquired by crawling.
OUTPUT:	Cyber Security Domain Analytics

7.3 Continuous Risk Monitoring Module (CRMM)

Continuous Risk Monitoring Module (CRMM) assesses on a continuous basis the performance of the implemented risk-reducing cyber security controls allowing the adaptation of the cyber insurance contract to the changing IT environment and the evolving cyber threat landscape. CRMM will serve as mediator between insurance companies that offer cyber insurance coverage and future clients in order to optimize this process. CRMM will offer invaluable quantitative metrics and qualitative insights of an organization's risk. In addition, CRMM will calculate and simulate how risk might propagate and manifest itself on multiple assets across your organizational structure to determine the total risk level and the potential impact of a current risk controls' failure. Operational risk management is a constant and systematic process that must be performed firstly top-down, i.e. at a high level, in order to identify the key risks, and at the bottom-up, i.e. at a low level, to identify all risks in more detail. In both approaches the same steps are followed in the process of risk management, and the difference lies in the degree of thoroughness. The continuous risk monitoring module will periodically scan the organization's assets and relations between those assets. Another feature of the continuous risk monitoring module is the continuous periodical update of the vulnerabilities database from NIST's database (through the BDCPM). In addition, the CRMM will directly feed the SECONDO blockchain for

as an immutable way to record risk values.

Table 16 Input/output CRMM

INPUT:	Harmonized Metamodel, Analytics
OUTPUT:	Risk Assessment

7.4 Cyber Security Investment Module (CSIM)

Cyber Security Investment Module (CSIM) is empowered by a game-theoretic approach, which is used to model defending-attacking scenarios and derive optimal defense strategies in the presence of attackers that aim to cause maximum damage. Costs for attacking and defending will be investigated and they will be given as an input to CSIM. The latter will take as inputs: (a) the outcome of the provided QRAM, and (b) the results of BDCPM that provides analytics on Internet sources regarding state-of-the-art security solutions as well as their cost. All inputs modelled and processed by CSIM will provide recommendations for optimal investments in cyber security. To take into account cyber insurance, CSIM will provide decision support for organizations that seek an optimal equilibrium point (i.e. balance) between spending on cyber security investment and cyber insurance fees. The two complementary modules are the Game Theoretic (GTM) and the Econometrics Module (ECM):

7.4.1 Game Theoretic Module (GTM)

Game Theoretic Module (GTM) models all possible attacking scenarios and defensive strategies, (i.e. available security controls), by employing attack graphs. GTM will use a Bayesian game-theoretic approach to model interactions between the defending organization and an attacker that can achieve maximum damage to system. Then game-theoretic techniques will be used to derive optimal defending strategies in the form of Nash Equilibria (NE). It will also use semantic reasoning algorithms and methodologies, based on ontological information models, for the recommendation of optimal countermeasures to defend against identified vulnerabilities and threats CRMM will feed directly, with the risk output, the GTM module for further analysis. More specifically, a series of techniques will be developed to construct high-level attack scenarios. This approach will integrate complementary proactive defense methods and use the intrinsic relationships between possibly related attacks to hypothesize and reason. Particularly we will focus in two types of proactive defense methods: proactive defense based on prerequisites and consequences and proactive defense based on similarity. Defining what proactive and reactive is, proactive is method used which provides security before an incident occurs. Reactive security is another type of security method which provides security at the time of the occurrence of a cybersecurity attack (ex. IDS). Proactive security based on prerequisites and consequences is a type of tool which requires input and provides output based on the current condition of an organization with the goal to limit the risks that the organization faces (ex. Risk assessment tool). Proactive defense based on similarity will acquire data from our BDCPM and use pattern matching techniques that will be developed throughout the project to provide with us possible attacks patterns and risks [131]. These two methods correlate alerts using different mechanisms, combining them can potentially lead to better correlation results. These techniques are critical to constructing high level attack scenarios. Moreover, to reason about hypothesized attacks, we will develop techniques to compute constraints that indirectly related attacks must satisfy and proposed to further validate hypothesized attacks through raw audit data. In the context of this

module, a two-stage model will be designed to aid security managers with decisions regarding the optimal allocation of a cyber security budget with the option to outsource risk to a cyber insurer. GTM will interface these models with risk analysis (precursor step) and the cyber insurance (successor step) in a complete business process.

Table 17 Input/output GTM

INPUT:	Risk Assessment, Analytics
OUTPUT:	Optimal Defending Strategies

7.4.2 Econometrics Module (ECM)

This module will use the asset pricing methods proposed. Asset pricing is the procedure of adding economical tags on every asset that an organization owns and has financial loss or gain from its state. In financial economics, asset pricing refers to a formal treatment and development of two main pricing principles [133] a) the general equilibrium asset pricing and the b) rational pricing. SECONDO will use existing the asset pricing methods to support the functionalities of ECM sub-module will providing e an estimate of pricing for each organizations' assets. The asset pricing models are necessary in determining the asset-specific required rate of return on investment, or in pricing derivatives on these for trading or hedging. For intangible assets, we intend to use cross sectional analysis of large numbers of organizations (using the ORBIS global database and some primary data generated within the project) to construct upper and lower bounds on the value of the intangible. An asset is defined as an economic source of value, that is, it is any resource of economic value that an entity owns or controls with the expectation that it will lead to a benefit in future. The management of an asset throughout its lifecycle is crucial for guaranteeing a favorable return and ensuring defined services and operations. The Econometrics Module (ECM) will provide estimations of all kinds of costs of potential attacks and it takes into account costs, (i.e. purchase, installation, execution, etc.), of each possible security control using a set of existing econometric models. Firstly, we model the scenario as a one-shot game that aims to optimize the defense including direct costs, and secondly a Knapsack problem that considers only pure strategies for each control level including indirect costs. We compute the Nash Equilibrium condition in Control Games, and we motivate the trade-offs required with the indirect costs. The solution to each control-game alone is insufficient in dictating the optimal allocation of an organization's cybersecurity budget. So, to identify the best way to allocate a budget, we formalize the problem as a multi-objective multiple-choice Knapsack problem [132]. Current trends indicate that IT security measures will need to greatly expand to counter the ever increasingly sophisticated, well-funded and/or economically motivated threat space. Complementary to this module will be the module mentioned before (GTM) which will calculate all the possible attack scenarios which in turn get calculated in monetary amount in this module. Moreover, having into consideration the continuous risk monitoring module (CRMM) these indications will be efficient and easily translated to cyber security insurance coverage required to fully mitigate the underdeveloped risk. Last but not lease, ECM will also consider ORBIS global database and some primary data generated within the project produce the costs.

Table 18 Input/output ECM

INPUT:	Risk Assessment, Orbis DB, SECONDO produced data, Analytics
OUTPUT:	Costs

7.5 Cyber Insurance Coverage and Premiums Module (CICPM)

The Cyber Insurance Coverage and Premiums Module (CICPM) will compute premium curves and coverages as a function of the organization's security level. These can be used by clients to determine desirable levels of cyber security investment prior to any cyber insurance contract agreement. CICPM will follow a standardized logic, which enables underwriters to incorporate their own strategy, as required by a competitive market; and, on the other hand, minimizes the information asymmetry between insurer and insured. This module will take input from CSIM module it's produced reports, as well as the analytics produced by the BDCPM module. CICPM will provide insurance exposure assessment and estimates insurance coverage and premiums based on the insurance policy of the underlying insurer, which will be modelled and incorporated using a new developed cyber insurance ontology. Privacy-preserving smart contracts will be leveraged to hide sensitive client information. This task will also provide the organization and clients flexible smart contract description, so that more expressive contract contents are reflected in the digital format of the insurance. To achieve its goals, the proposed insurance calculation tool will take input from: a) the CRMM for monitoring the conditions that violate cyber insurance contract agreements toward resolving conflicts; b) the defending policies selected to be applied in order to provide optimal protection strategies as well as the results of the related econometric parameters that justify the cost effectiveness of the considered security investments; c) analytics on cyber insurance environment and market; and d) the underwriter's strategy. In order to provide a standardized and verifiable insurance calculation model in the form of smart contract.

Table 19Input/output CICPM

INPUT:	Risk Assessment, Costs, Strategies, Analytics
OUTPUT:	Cyber insurance premiums and coverage

7.6 Blockchain and Smart Contracts

SECONDO will deploy a private Ethereum blockchain, which is a distributed decentralized database that maintains continuously growing blocks of data records, in which all blocks are tightly chained together against information tampering. The private ledger is necessary to provide secure access control on data records, to hold an inventory of assets and information regarding security and privacy risk measurable indicators of an organization (cyber insurance client). We chose the private ledger because we need to keep our transactions private and also to be able to control the functionality which is not the case on public ledger [134].Thus, risk is efficiently ceded or retroceded through smart contracts embedded in the distributed ledger specifically designed to process agreements and will notify parties when the agreement is bound and it then process premium and commission payments. The ledger will be updated based on information received from CRMM. Due to the immutability of the ledger, the organization cannot modify a declaration, which has been already stored in the ledger, to earn more credit on insurance claim. By using smart contracts, fraud is restricted as only valid claims

are recognized. Privacy-preserving techniques will be used in data storage and smart contracts to protect clients' privacy. Privacy-preserving smart contracts for insurance coverage will be leveraged to hide sensitive client information. A smart contract has an account balance, a private storage and executable code. The contract's state comprises the storage and the balance of the contract. The state is stored on the blockchain and it is updated each time the contract is invoked. There are two types of smart contracts, namely, deterministic and non-deterministic smart contracts. A deterministic smart contract is a smart contract that when it is run, it does not require any information from an external party (from outside the blockchain). A non-deterministic smart contract is a contract that depends on information (called oracles or data feeds) from an external party. In the context of SECONDO, a non-deterministic approach will be used as we require communication of the smart contract with all other SECONDO components.

Table 20 Input/output Blockchain

INPUT:	Risk Assessment, Insurance Smart Contracts
OUTPUT:	Immutable Stored Information

8 Candidate Implementation Technologies

In this chapter, we try to elaborate on the technical approach that will be followed in order to realize the functionalities described in this document and to implement the components that constitute the SECONDO framework. The final SECONDO Integrated platform will be delivered at the end of M42. The sub sections below provide a brief description of the provision of technologies selected for the SECONDO framework implementation. Table and Figure below highlights the provision of technologies to be used per component, while the following subsections provide a small summary on these selected technologies.

Table 21 Technologies per component

Component	Technologies
Quantitative Risk Analysis Metamodel (QRAM)	CORAS Method
Continuous Risk Monitoring Module (CRMM)	OLISTIC Enterprise Risk Management
Cyber Insurance Coverage and Premiums Module (CICPM)	Ethereum private blockchain & Smart Contracts (e.g. solidity)
Big Data Collection and Processing Module (BDCPM)	Apache Spark, Python, ELK (Elastic, Logstash, Kibana)

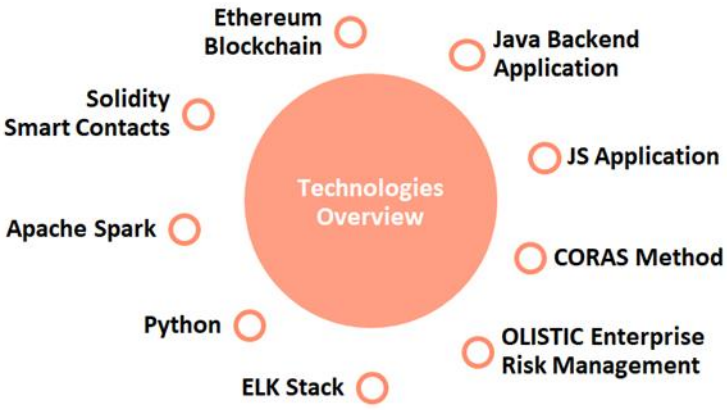

Figure 6 SECONDO Technologies

8.1 Blockchain and Smart Contracts

Ethereum [135] is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract (scripting) functionality for decentralized applications. Ethereum has a native cryptocurrency called Ether (ETH). Ether is a cryptocurrency generated by the Ethereum platform and used to compensate mining nodes for computations performed. Each Ethereum account has an ether balance and ether may be transferred from one account to another. Ethereum provides a decentralized virtual machine, the Ethereum Virtual Machine (EVM), which can execute scripts using an international network of public nodes. The virtual machine's instruction set, in contrast to others like Bitcoin Script, is thought to be Turing-complete. "Gas", an internal transaction pricing mechanism, is used to mitigate spam and allocate resources on the network. Unlike other blockchains, Ethereum is programmable, which means that developers can use it to build new kinds of applications. These decentralized applications (or “dapps”) gain the benefits of cryptocurrency and blockchain technology. Ethereum, defines a set of generalized protocols which have become the pillars of the development of decentralized applications. As already mentioned, at the heart of this, lies the EVM. The Figure 3 below explains the architecture. The Ethereum Virtual Machine is not only completely sandboxed, but also completely isolated. This means that code that is currently running on the EVM has no access to the network or the filesystem and can sparingly access other contracts.

Ethereum's smart contracts are based on different computer languages, which developers use to program their own functionalities. Smart contracts are high-level programming abstractions that are compiled down to EVM bytecode and deployed to the Ethereum blockchain for execution. They can be written in Solidity (a language library with similarities to C and JavaScript), Serpent (similar to Python, but deprecated), LLL (a low-level Lisp-like language), and Mutan (Go-based, but deprecated). There is also a research-oriented language under development called Vyper (a strongly typed Python-derived decidable language).

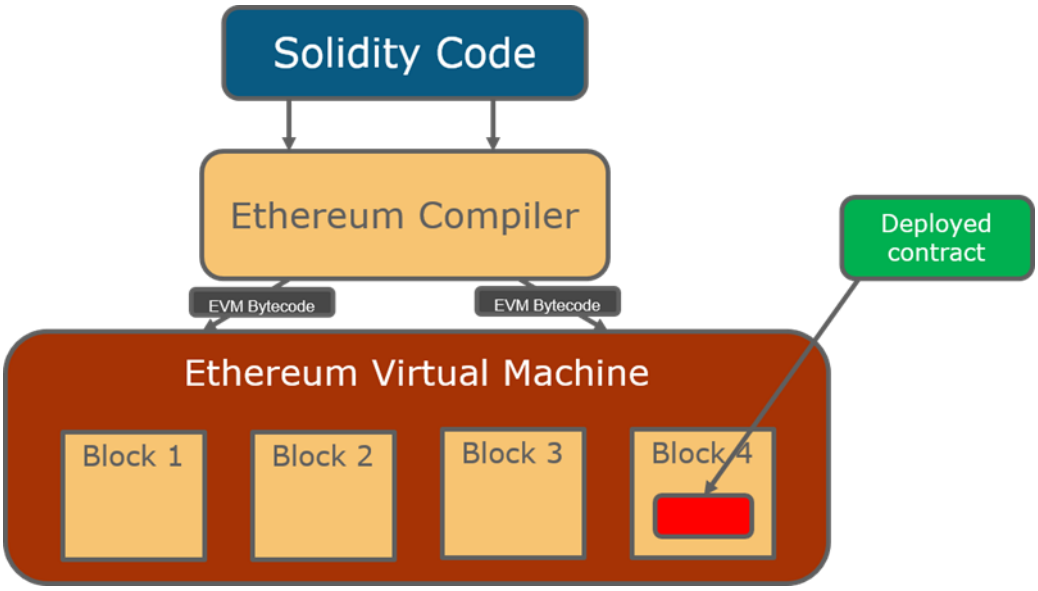

Figure 7 SECONDO Technologies

Ethereum is the leading blockchain among enterprises. For instance, more than 50% of the billion-dollar firms included in Forbes' "Blockchain 50: Billion Dollar Babies" list are building applications on top of Ethereum or deriving platforms from it. SECONDO will be based on Ethereum for the following reasons:

- First mover advantage: Ethereum is the first programmable blockchain that features a Turing-complete language on its blockchain that features smart contract functionality.

- It's a well-planned project: The majority of cryptocurrencies are quite spontaneous, appearing and dying quickly. Ethereum, on the other hand, is a project with a high level of credibility based on its lasting history — in comparison to other crypto projects — with its white paper released in 2013 and its launch in 2015.

- It has massive support: Ethereum has the largest community of developers working on its blockchain protocol. Hundreds of thousands of developers are working on the Ethereum ecosystem, and the project is backed by both medium-sized companies and large corporations. Also, the Ethereum Enterprise Alliance and Hyperledger monitor and contribute to the development of the project continually.

- Rapid deployment: It's easy for developers and enterprises to get started with Ethereum. All-in-one BaaS platforms like Microsoft Azure and Amazon Managed Blockchain services and software-as-a-service (SaaS) platforms like ConsenSys-backed Kaleido attempt to make it easy for businesses to develop their own blockchain networks. New tools and development kits are continuously being released so that Ethereum can easily be adopted among enterprises and businesses.

- Interoperability: Enterprises can develop Ethereum-based private/permissioned blockchain networks and plug them into the public Ethereum mainnet to enjoy the vast, active, high-value public blockchain and all the parts of its ecosystem. An example of this is Pantheon from PegaSys, which is

Ethereum's first enterprise client that is compatible with the public chain. All in all, Ethereum's interoperability essentially keeps enterprise blockchains up to date, as it offers them global reach, an expansive network of users and DApps, and continuous developments and upgrades.

8.2 Risk Managements (Modelling and Analysis)

CORAS [136] is a method for conducting security risk analysis. CORAS provides a customised language for threat and risk modelling and comes with detailed guidelines explaining how the language should be used to capture and model relevant information during the various stages of the security analysis. The language consists of five different kinds of diagrams: asset diagrams, threat diagrams, risk diagrams, treatment diagrams, and treatment overview diagrams. In this respect CORAS is model based. The Unified Modelling Language (UML) is typically used to model the target of the analysis. For documenting intermediate results, and for presenting the overall conclusions we use special CORAS diagrams which are inspired by UML. The CORAS method provides a computerised tool designed to support documenting, maintaining and reporting analysis results through risk modelling. In the CORAS method a security risk analysis is conducted in eight steps (see Figure below). SECONDO will be based on the CORAS method since it allows the integration of several different risk assessment processes, is easily extensible and is based on the ISO 31000 risk management standard. Compared to other approaches such as CRAMM and OCTAVE, that rely on text and tables, CORAS uses diagrams as an important means for communication, evaluation and assessment.

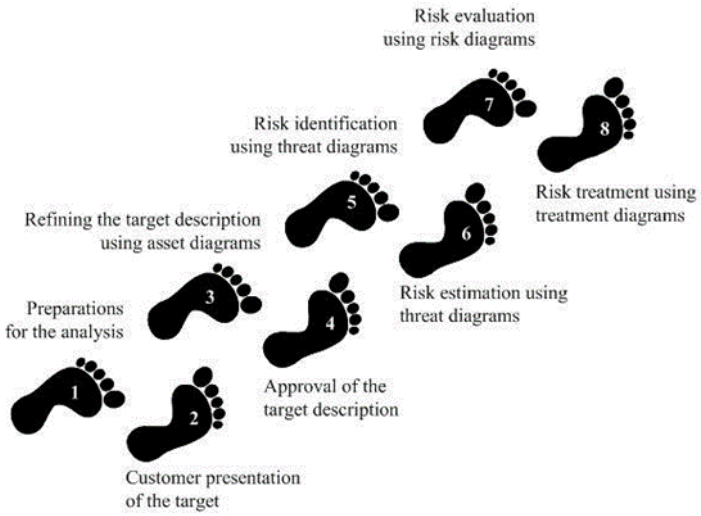

Figure 8 CORAS security risk analysis steps

The main CORAS result is the CORAS framework for model-based risk assessment. As illustrated in Figure 5, the CORAS framework has four main anchor points, a) A risk management process, b) A risk documentation framework, c) An integrated risk management and development process and d) A platform for tool-inclusion based on data integration.

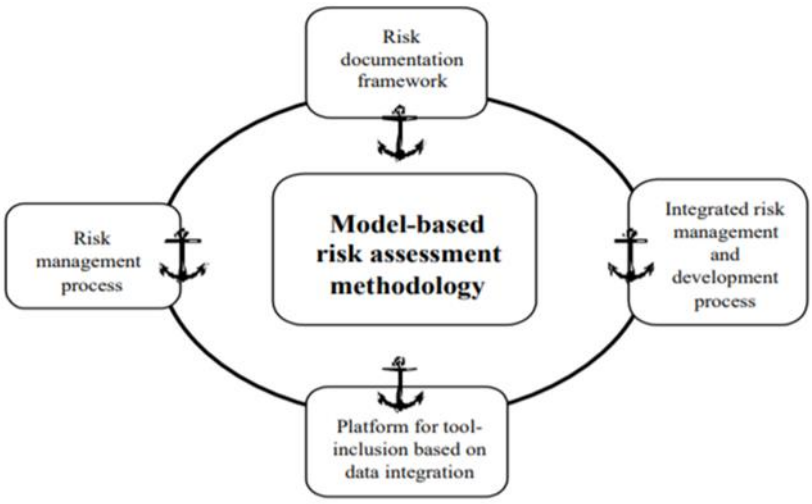

Figure 9 The CORAS framework for model-based risk assessment

OLISTIC Enterprise Risk Management [137] suite performs dynamically, continuously and near-real time cyber-physical security risk assessment in compliance to the ISO/IEC 27001 standard on information security management, as well as privacy risk assessment according to the General Data Protection Regulation (GDPR), addressing the various possible cascading effects that are associated with security incidents occurring from interacting entities and assets. As risk assessment is a complex and data-rich process, OLISTIC enables organizations to define, graphically represent and document all cyber-physical assets of them within the scope of the security risk assessment process, as well as to specify the dependencies among several assets and link each asset with (multiple) predefined threats and vulnerabilities, denoting their likelihood and resulting impacts, together with details of the assets ownership and their confidentiality classification. Having outlined the organization's assets structure accompanied with their threats and vulnerabilities, a continuous risk assessment process initiates highlighting the cyber-physical risks of the organization's infrastructure and proposing countermeasures though the instantiation of predefined security policies (derived from widely adopted international standards, such as the ISO 27001) to mitigate the identified risks - taking into consideration (near-real-time continuous risk assessment) any changes on the organization's assets structure and any updates on the threats' cascading models and effects, which the organization may dynamically introduce in the security risk assessment process (dynamic asset management). OLISTIC is sophisticated global risk assessment framework that can deal with cascading effects risks, threats and vulnerabilities. It adopts the aforementioned innovative and novel mathematical models (e.g. graph theory) to derive the overall and cascading risks and to identify the most appropriate security controls in order to deal with those security threats that exhibit the highest risk, as well as to thwart cascading risks which rise due to the inter-dependencies. In the context of SECONDO, OLISTIC (UBITECH's product) will be enhanced and extended to support optimal security investments and estimate also cyber insurance premiums. The following Figure demonstrates an overview of the OLISTIC results.

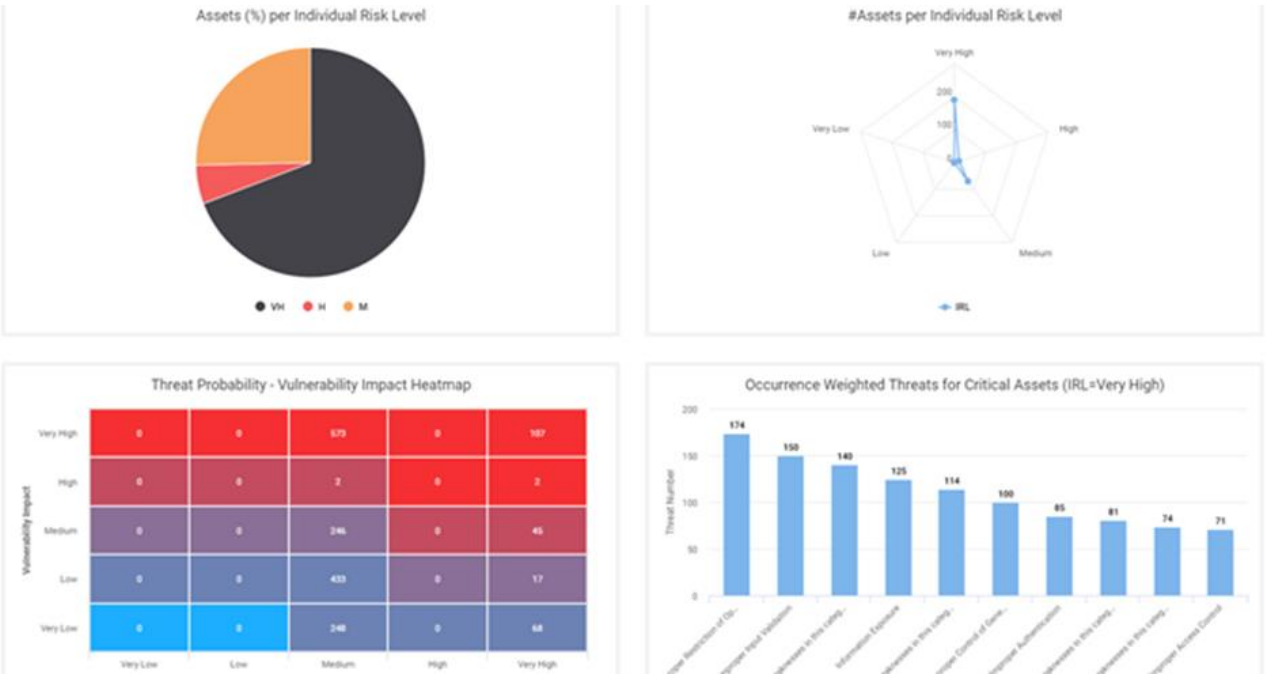

Figure 10 OLISTIC Results

8.3 Data Processing and ELK Stack

Apache Spark [138] is a unified analytics engine for large-scale data processing. More specifically, is an open-source distributed general-purpose cluster-computing framework. Spark provides an interface for programming entire clusters with implicit data parallelism and fault tolerance. Spark Core is the foundation of the overall project. It provides distributed task dispatching, scheduling, and basic I/O functionalities, exposed through an application programming interface (for Java, Python, Scala, and R) centred on the RDD abstraction. In the context of SECONDO Python language will be used. Spark Streaming uses Spark Core's fast scheduling capability to perform streaming analytics. It ingests data in mini-batches and performs RDD transformations on those mini-batches of data. This design enables the same set of application code written for batch analytics to be used in streaming analytics, thus facilitating easy implementation of lambda architecture.

Apart from Apache Spark, ELK Stack will be used. "ELK" is the acronym for three open source projects [141] : Elasticsearch, Logstash, and Kibana. Elasticsearch is a search and analytics engine. Logstash is a server-side data processing pipeline that ingests data from multiple sources simultaneously, transforms it, and then sends it to a "stash" like Elasticsearch. Kibana lets users visualize data with charts and graphs in Elasticsearch. SECONDO will also use this stack for data processing and search. ELK Stack is chosen since it is open source, easy to set up and manage, while performance optimization, and scalability are handled automatically. But the biggest feature of the elasticsearch database is the speed that can query such huge amounts of data, which in our case is essential for our project.

Figure 11 ELK

8.4 SECONDO Platform Implementation

Java Spring Boot [139] is an application framework and inversion of control container for the Java platform. The framework's core features can be used by any Java application, but there are extensions for building web applications on top of the Java EE (Enterprise Edition) platform. Although the framework does not impose any specific programming model, it has become popular in the Java community as an addition to, or even replacement for the Enterprise JavaBeans (EJB) model. The Spring Framework is open source.

9 Conclusions

Deliverable 2.1 is fundamental to the subsequent stages of SECONDO for several reasons: (i) it defines the usage scenarios where the initial technical requirements are going to be extracted from; (ii) it provides a means of verification and evaluation of the final system; and (iii) it ascertains that all involved stakeholders are represented and heard upon when it comes to their individual requirements.

The use case scenarios for SECONDO were driven by the partners and supported by the technology providers in defining the most relevant services which together will make the SECONDO platform. Four use cases made up of four scenarios that have been defined along with the modules involved the analysed use cases are presented in such a way to express the functionality and to elicit the core functionalities of SECONDO. In addition, an important outcome of this analysis is the identification of possible issues and benefits feeding into the list of requirements. The SECONDO architecture presents the modules of the system and technologies used to communicate between them, while also taking into account business case and system requirements. SECONDO architecture utilizing the above technologies achieves its goals providing an integrated platform. The reference architecture is the basis for the design and the implementation of the technical solutions for SECONDO.

10 References

[1] "Guide for Conducting Risk Assessments," National Institute of Standards and Technology (NIST)Special Publication 800-30/Computer Security Division, 2012.

[2] A.Shameli-Sendi, R.Aghababaei-Barzegar, M.Cheriet, "Taxonomy of information security risk assessment (ISRA)," *Computers & security,* vol. 57, pp. 14-30, 2016.

[3] T.Sommestad, M.Ekstedt, P.Johnson, "A probabilistic relational model for security risk analysis," *Computers & Security,* vol. 29, no. 6, pp. 659-679, 2010.

[4] R.Oppliger, "Quantitative risk analysis in information security management: a modern fairy tale.," *IEEE Security & Privacy,* vol. 13, pp. 18-21, 2015.

[5] A.Ekelhart, S.Fenz, M.Klemen, E.Weippl, "Security ontologies: Improving quantitative risk analysis," in *IEEE/40th Annual Hawaii International Conference on*, 2007.

[6] A.Avizienis, J.C.Laprie, B.Randell, C.Landwehr, "Basic concepts and taxonomy of dependable and secure computing.," *IEEE transactions on dependable and secure computing,* pp. 11-33, 2004.

[7] A.Singhal, D.Wijesekera, "Ontologies for modeling enterprise level security metrics," in *In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research/ACM*, 2010.

[8] "ENISA Threat Landscape Report 2017," 2018. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017. [Accessed November 2019].

[9] "Risk Assessment - Quantitative Methods," CorpsRisk Analysis Gateway Training Module/Institute for Water Resources/US Army Corps of Engineer.

[10] F.J.Groen, C.Smidts, A.Mosleh, "QRAS—the quantitative risk assessment system," *Reliability Engineering & System Safety,* vol. 91, no. 3, pp. 292-304, 2006.

[11] F.J.Groen, C.S.Smidts, A.Mosleh, S.Swaminathan, "QRAS - The Quantitative Risk Assessment System," in *IEE*, 2002.

[12] "Quantitative Risk Assessment System (QRAS) / Inventors: R.M Weinstock, C.S. Smidts, A. Mosleh, Y. Chang, S.Swaminathan, F.J.Groen, Z.Tan, Zhibin". NASA Technical Reports Server Patent 20080004905, 2001.

[13] A.Mosleh, P.J.Rutledge, F.J.Groen, "Quantitative Risk Assessment System (QRAS) for Space Mission PRA," *Joint ESA-NASA Space-Flight Safety Conference. Edited by B. Battrick and C. Preyssi. European Space Agency, ESA SP-486, ISBN: 92-9092-785-2., p.101,* 2002.

[14] L.Rajbhandari, E.Arthur Snekkenes, "Mapping between Classical Risk Management and Game Theoretical Approaches," in *Springer, pages 147–154*, Berlin, 2011.

[15] D.Liu, X.Wang, J.Camp, "Game-theoretic modeling and analysis of insider threats," *International Journal of Critical Infrastructure Protection,* vol. 1, pp. 75-80, 2008.

[16] J.P.Herbert, J.Yao, "Game-Theoretic Risk Analysis in Decision-Theoretic Rough Sets," in *Springer International Conference on Rough Sets and Knowledge Technology*, 2008.

[17] Z.Ismail, J. Leneutre, D.Bateman, L.Chen, "A Game-Theoretical Model for Security Risk Management of Interdependent ICT and Electrical Infrastructures," in *IEEE*, 2015.

[18] S.Musman, A.Turner, "A game theoretic approach to cyber security risk management," *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology,* vol. 15, no. 2, pp. 127-146, 2018.

[19] "Continuous Monitoring of Third Party Vendors: Building Best Practices," The Santa Fe Group, Shared Assessments Program, 2017.

[20] M.A.Vasarhelyi, "The Coming Age of Continuous Assurance," A condensed version of the 71st CPA Australia/University of Melbourne Annual, 2010.

[21] A.Smith, M.Papadaki, S.M.Furnell, "Improving awareness of social engineering attacks," in *Springer/ Information and Communication Technology*, Berlin, Germany, 2013.

[22] S. S. M. M. A.Karakasiliotis, "An assessment of end user vulnerability to phishing attacks," *Journal of Information Warfare,* vol. 6, no. 1, pp. 17-28, 2007.

[23] R. Dodge, A.Ferguson A, "Using Phishing for User Email Security Awareness’," in *Springer, Security and Privacy in Dynamic Environments*, 2006.

[24] Nolan and Levesque, "Hacking human: data-archaeology and surveillance in social networks," *ACM SIGGROUP Bulletin,* vol. 25, no. 2, pp. 33-37, 2005.

[25] G.L.Orgill, G.W.Romney, M.Bailey, P.Orgill, "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems," in *ACM Press/ Proceedings of 5th conference on IT education*, 2004.

[26] T.Bakhshi, M.Papadaki and S.M.Furnell, "A Practical Assessment of Social Engineering Vulnerabilities," in *Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance*, 2008.

[27] T.Greening, "Ask and Ye Shall Receive: A Study in ’Social Engineering," *ACM Press,* vol. 14, pp. 8-14, 1996.

[28] G.L.Orgill, G.W.Romney, M.G.Bailey, P.M. Orgill, "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems," in *ACM/Proceeding CITC5 '04 Proceedings of the 5th conference on Information technology education*.

[29] S.Jajodia, S. Noel, B. O’Berry, "Topological Analysis of Network Attack Vulnerability," in *247–266*, Boston, USA, 2005.

[30] X. Ou, S. Govindavajhala, A. W. Appel, "Mulval: A logic-based network security analyzer," in *Proceedings of the 14th Conference on USENIX Security Symposium,* Berkeley, CA, USA, 2005.

[31] "Skybox security: Cybersecurity management analytics.," [Online]. Available: https://www.skyboxsecurity.com/.

[32] "Redseal network risk scoring," [Online]. Available: https://www.redseal.net.

[33] "Nessus professional vulnerability scanner," [Online]. Available: https://www.tenable.com.

[34] "Nmap: the network mapper - free security scanner," [Online]. Available: https://nmap.org/.

[35] "Retina network security scanner," [Online]. Available: https://www.beyondtrust.com.

[36] V. Mehta, C. Bartzis, H. Zhu, E. Clarke, J. Wing, "Ranking attack graphs,” in Recent Advances in Intrusion Detection," in *Springer,* Berlin Heidelberg, 2006.

[37] A. Singhal, X. Ou, "Security risk analysis of enterprise networks using probabilistic attack graphs," in *Network Security Metrics*, Springer, 2017, pp. 53-73.

[38] B.Zoullouti, M.Amghar, S.Nawal, "Using Bayesian Networks for Risk Assessment in," in *Advances and Novel Applications*, 2019, pp. 39-53.

[39] C.A. Pollino, O.Woodberry, A.Nicholson, "Parameterisation and evaluation of a Bayesian network for use in an ecological risk assessment," *Environmental Modelling & Software,* vol. 22, no. 8, pp. 1140-1152, 2007.

[40] D.Hanea, R.Cooke, B.Ale, "The methodology to build the network used in a Bayesian Belief Net approach," in *In Proceedings of the eighth international conference PSAM*, New Orleans, Louisiana, USA, 2006.

[41] WP.Aspinall, G.Woob , B.Voight, "Evidence-based volcanology:application to eruption crises," Penn State University(department of geosciences), Cambridge University(Department of Public Health and Primary Care), 2003.

[42] L. A. a. L. M. P. Gordon, "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC),* vol. 5, no. 4, pp. 438-457, 2002.

[43] M. a. R. J. a. C. A. a. C. J. Gupta, "Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach," *Decision Support Systems,* vol. 41, pp. 592-603, 2006.

[44] L. P. a. D. J. K. a. R. T. R. a. B. W. H. Rees, "Decision support for cybersecurity risk planning," *Decision Support Systems,* vol. 51, no. 3, pp. 493--505, 2011.

[45] T. R. a. D. J. K. a. R. L. P. Rakes, "IT security planning under uncertainty for high-impact events," *Omega: International Journal of Management Science,* vol. 40, pp. 79-88, 2012.

[46] J. K. a. R. C. T. a. R. T. R. a. R. L. P. Deane, "Managing supply chain risk and disruption from IT security incidents," *Operations Management Research,* vol. 2, pp. 1-4, 2009.

[47] V. a. M. C. a. H. W. a. L.-P. D. Viduto, "A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem," *Decision Support Systems,* vol. 53, pp. 599-610, 2012.

[48] T. Sawik, "Selection of optimal countermeasure portfolio in IT security planning," *Decision Support Systems,* vol. 55, pp. 156-164, 2013.

[49] R. J. a. S. R. Kauffman, "Risk management of contract portfolios in IT services: The profit-at-risk approach," *Journal of Management Information Systems,* vol. 25, pp. 17-48, 2008.

[50] Y. J. a. K. R. J. a. S. R. Lee, "Profit-maximizing firm investments in customer information security," *Decision Support Systems,* vol. 51, no. 904-920, p. 2011.

[51] A. a. D. P. a. S. S. Nagurney, "A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints," *Annals of operations research,* vol. 248, pp. 405-427, 2017.

[52] B. a. Y. J. a. T. G. K. Srinidhi, "Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors," *Decision Support Systems,* vol. 75, pp. 49-62, 2015.

[53] H. a. S. R. a. W. T. Cavusoglu, "Decision-theoretic and game-theoretic approaches to IT security investment," *Journal of Management Information Systems,* pp. 281-304, 2008.

[54] L. a. B. D. Demetz, "To Invest or Not to Invest? Assessing the Economic Viability of a Policy and Security Configuration Management Tool," *The Economics of Information Security and Privacy,* pp. 25-47, 2013.

[55] F. a. M. P. Smeraldi, "How to spend it: optimal investment for cyber security," *Proceedings of the 1st International Workshop on Agents and CyberSecurity,* p. 8, 2014.

[56] M. a. M. P. Cremonini, {Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA), Cambridge, MA, USA: Proceedings of the 4th Workshop on the Economics of Information Security, 2005.

[57] J. a. C. A. a. R. R. H. Wang, "Research Note-A Value-at-Risk Approach to Information Security Investment," *Information Systems Research,* pp. 106-120, 2008.

[58] A. a. P. E. a. M. P. a. H. C. a. S. F. Fielder, "Game theory meets information security management," in *Proc. of the 29th IFIP International Information Security and Privacy Conference*, 2014.

[59] A. a. P. E. a. M. P. a. H. C. a. S. F. Fielder, "Decision support approaches for cyber security investment," *Decision Support Systems,* vol. 86, pp. 13-23, 2016.

[60] A. a. K. S. a. P. E. a. S. S. a. R. S. Fielder, "Risk assessment uncertainties in cybersecurity investments," *Game,* vol. 9, p. 34, 2018.

[61] S. S. Wang, "Integrated framework for information security investment and cyber insurance," *{Pacific-Basin Finance Journal,* vol. 57, p. 101173, 2019.

[62] M. a. P. E. a. G. J. Chronopoulos, "An options approach to cybersecurity investment," *IEEE Access,* vol. 57, pp. 12175--12186, 2017.

[63] R. a. L. G. Heartfield, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," *ACM Computing Surveys,* vol. 78, p. 37, 2016.

[64] J. A. a. W. X. Paul, "Socially optimal IT investment for cybersecurity," *Decision Support Systems,* 2019.

[65] A. a. A.-S. E. Dutta, "Cyber defense matrix: a new model for optimal composition of cybersecurity controls to construct resilient risk mitigation," *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security,* 2019.

[66] F. a. U. G. a. Y. A. Martinelli, "Optimal Security Configuration for Cyber Insurance," *IFIP International Conference on ICT Systems Security and Privacy Protection,* no. 2018, pp. 187--200.

[67] M. Eling, "Cyber risk and cyber risk insurance: status quo and future research," 2018.

[68] M. A. a. B. R. Henk, "Blockchain: An insurance focus," 2019.

[69] K. DiGrazia, "Cyber Insurance, Data Security, and Blockchain in the Wake of the Equifax Breach," *J. Bus. & Tech. L,* vol. 13, p. 255, 2017.

[70] O. A. Mohamed, "E-Insurance Concept, Importance and Applications".

[71] S. a. X. Z. a. N. D. a. W. P. a. W. S. S. a. Z. Y. Feng, "Cyber Risk Management with Risk Aware Cyber-Insurance in Blockchain Networks," in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1-7.

[72] T. a. C. G. a. E. K. Lepoint, "BlockCIS—A blockchain-based cyber insurance system," *2018 IEEE International Conference on Cloud Engineering (IC2E),* pp. 378-384, 2018.

[73] I. a. B. S. a. S. S. Vakilinia, "Crowdfunding the Insurance of a Cyber-Product Using Blockchain," *Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON).*

[74] A.Marotta, F.Martinelli, S.Nannia, A.Orlando, A.Yautsiukhin, "Cyber-insurance survey," *Computer Science Review,* vol. 24, pp. 35-61, 2017.

[75] "Sigma, Swiss Re Institute," 1 November 2017. [Online]. Available: https://www.swissre.com/dam/jcr:995517ee-27cd-4aae-b4b1-44fb862af25e/sigma1_2017_en.pdf. [Accessed 10 December 2019].

[76] Young, D., Lopez Jr, J., Rice, M., Ramsey, B., & McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. International Journal of Critical Infrastructure Protection, 14, 43-57.

[77] R.P. Majuca, W.Yurcik, J.P. Kesan, "The Evolution of Cyberinsurance," Technical Report CR/0601020, ACM Computing Research Repository, 2006.

[78] W.S. Baer, A. Parkinson, "Cyberinsurance in it security management," *IEEE Security & Privacy ,* vol. 5, no. 3, pp. 50-56, 2007.

[79] D.Woods, I.Agrafiotis, J.R.C.Nurse, S.Creese, "Mapping the coverage of security controls in cyber insurance proposal forms," *Journal of Internet Services and Applications,* 2017.

[80] M.Lelarge, J.Bolot, "A local mean field analysis of security investments in networks.," in *ACM, In Proceedings of the 3rd international workshop on Economics of networked systems*, 2008.

[81] M.Lelarge, J.Bolot, "Network externalities and the deployment of security features and protocols in the internet.," *ACM SIGMETRICS Performance Evaluation Review,* vol. 36, no. 1, pp. 37-48, 2008.

[82] R.Pal, L.Golubchik, "Analyzing self-defense investments in internet security under cyber insurance coverage," in *30th International Conference on IEE, In Distributed Computing Systems (ICDCS)*, 2010.

[83] "Managing Cyber Insurance Accumulation Risk," Cambridge Centre for Risk Studies and Risk Management Solutions, Cyber Accumulation Risk Management working paper, 2016.

[84] "Cyber Exposure Data Schema v1.0," Cambridge Centre for Risk Studies and Risk Management Solutions, Cyber Accumulation Risk Management working paper, 2016.

[85] "ENISA Threat Landscape Report 2017," 15 January 2018. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017. [Accessed 10 December 2019].

[86] "ENISA, Cyber Insurance: Recent Advances, Good Practices and Challenges," 07 November 2016. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges. [Accessed 10 December 2019].

[87] "ENISA, NCSS Good Practice Guide," 14 November 2016. [Online]. Available: https://www.enisa.europa.eu/publications/ncss-good-practice-guide. [Accessed 10 December 2019].

[88] S. Romanosky, "Examining the costs and causes of cyber incidents”," *Journal of Cybersecurity,* 2016.

[89] "Enhancing the Role of Insurance in Cyber Risk Management,OECD Publishing, Paris," 08 December 2017. [Online]. Available: https://doi.org/10.1787/9789264282148-en. [Accessed 10 December 2019].

[90] A.Marotta, F.Martinelli, S.Nanni, A.Orlando, A.Yautsiukhin, "Cyber-insurance survey," *Computer Science Review,* 2017.

[91] "Cyber Insurance and Systemic Market Risk/EastWest Institute," 2019. [Online]. Available: https://www.eastwest.ngo/sites/default/files/ideas-files/cyber-insurance-and-systemic-market-risk.pdf. [Accessed 10 December 2019].

[92] "PwC Global Cyber Insurance survey," 2018. [Online]. Available: https://www.pwc.com/us/en/industry/assets/pwc-cyber-insurance-survey.pdf. [Accessed 10 December 2019].

[93] N.Szabo, "Smart Contracts: Building Blocks for Digital Markets," 1996. [Online]. Available: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

[94] "The Idea of Smart Contracts," 1997. [Online]. Available: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html. [Accessed 2019].

[95] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 5 December 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed 2019].

[96] G.Ciocarlie, K.Eldefrawy, T.Lepoint, "BlockCIS—A Blockchain-based Cyber Insurance System," in *2018 IEEE International Conference on Cloud Engineering*, 2018.

[97] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed December 2019].

[98] V.Buterin, "Ethereum: a next generation smart contract and decentralized application platform," 2013. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper. [Accessed December 2019].

[99] M.Bartoletti, L.Pompianu, "An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns," in *Financial Cryptography and Data Security*, Springer International Publishing, 2017.

[100] "Solidity source compiler," [Online]. Available: http://solidity.readthedocs.io/en/develop/installing-solidity.html.

[101] "Ethereum Wallet - MyCrypto," [Online]. Available: https://alterdice.com.

[102] "Ethereum Wallet - MyEtherWallet," [Online]. Available: https://www.myetherwallet.com/.

[103] "Ethereum Wallet - MetaMask," [Online]. Available: https://metamask.io.

[104] "Ethereum Wallet - MyCrypto," [Online]. Available: https://mycrypto.com/account.

[105] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, F.Y. Wang, "An overview of smart contract: architecture, applications, and future trends," *EEE Intelligent Vehicles Symposium (IV),* p. 108–113, 2018.

[106] M.Pustisek, A.Kos, "Approaches to front-end iot application development for the ethereum blockchain," *Procedia Computer Science,* vol. 129, p. 410–419, 2018.

[107] R.M Parizi, A.Dehghantanha, K.R.Choo, A.Singh, "Empirical vulnerability analysis of automated smart contracts security testing on blockchains," in *ACM, Proceedings of the 28th Annual International Conference on Computer Science and Software Engineering*, 2018.

[108] L.Luu, D.Chu, H.Olickel, P.Saxena, A.Hobor, "Making smart contracts smarter," in *In Proceedings of the 2016 ACM SIGSAC, Conference on Computer and Communications Security. ACM, 254–269*.

[109] B. Mueller, "Mythril," [Online]. Available: https://github.com/ConsenSys/mythril.

[110] Software Reliability Lab, "Security," [Online]. Available: https://securify.ch/.

[111] A.Mavridou,A.Laszka, "Tool demonstration: FSolidM for designing secure Ethereum smart contracts.," in *In International Conference on Principles of Security and Trust. Springer, 270–277*, 2018.

[112] M. Wohrer, U. Zdun, "Smart contracts: security patterns in the Ethereum ecosystem and solidity," *Blockchain Oriented Software Engineering (IWBOSE),* 2018.

[113] C.Dannen, "Introducing Ethereum and Solidity," Springer, 2017.

[114] P.Praitheeshan, L.Pan, J.Yu, J. Liu, R.Doss, "Security Analysis Methods on Ethereum Smart Contract Vulnerabilities: A Survey," *Computer Science/ Published in ArXiv 2019.*

[115] H.Wang, Y.Wang, Z.Cao, Z.Li, G.Xiong, "An Overview of Blockchain Security Analysis," in *Springer, Communications in Computer and Information Science, China Cyber Security Annual Conference*, 2019.

[116] A.Kosba, A.Miller, E.Shi, Z.Wen, C.Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts.," *Security and Privacy ,* pp. 839-858, 2016.

[117] L.Luu, D.H.Chu, H.Olickel, P.Saxena, A.Hobor, "Making smart contracts smarter," in *In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016.

[118] R. &. S. G. (. J. M. C.-I. T. a. U. F. I. W. Böhme.

[119] G. P. a. C. N. 2. E. Cyber Insurance: Recent Advances.

[120] A. M. F. N. S. O. A. &. Y. A. (. C.-i. s. C. S. R. 2. 3.-6. Marotta.

[121] M. (. A. o. o. t. c. i. i. C. f. i. a. i. i. q. a. m. c. r. Payne.

[122] A. o. r. w. e. o. c. attack, "https://www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUSKCN1J231M".

[123] B. D. U. o. C.-I. F. R. Attack, "https://www.infosecurity-magazine.com/news/baltimore-buys-cyber-insurance/".

[124] M. F. $. M. F. F. 2. Mega-Breach, "https://www.forbes.com/sites/kateoflahertyuk/2019/07/09/marriott-faces-gdpr-fine-of-123-million/#1c1be6a14525".

[125] T. R. Report, "https://www.techriskreport.com/2019/02/recent-developments-yahoo-equifax-data-breach-litigation-suggest-increased-risk-personal-liability-directors-officers-cybersecurity-incidents/".

[126] T. C. I. A. $. M. P. v. $. M. (. F. I. Costs, "https://www.pbwt.com/data-security-law-blog/targets-cyber-insurance-a-100-million-policy-vs-300-million-so-far-in-costs/".

[127] 1. E. J. W. &. S. I. N. Y. Requirements Engineering: A Good Practice Guide.
[128] D. L. a. D. W. 1. M. S. R. A. U. Approach.
[129] R. a. L. G. a. B. S. a. B. A. a. F. J. R. a. F. A. a. R. E. Heartfield, "A taxonomy of cyber-physical threats and impact in the smart home," in *Computers & Security*, 2018, 398-428.
[130] P. a. D. R. D. a. C. S. a. M. R. M. a. N. R. a. H. M. Radanliev, "Economic impact of IoT cyber risk-analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance," 2018.
[131] S. A. Securing Infrastructure Facilities: When Does Proactive Defense Help-Manxi Wu.
[132] E. P. P. M. C. H. F. S. Decision support approaches for cyber security investment - Andrew Fieldera.
[133] J. H. Cochrane, Asset Pricing, vol. ISBN 0691121370., Princeton University Press, 2005.
[134] L. S. A. E. S. W. G. Trustless Blockchain-based Access Control in Dynamic Collaboration-Mouhamad Almakhour.
[135] Ethereum, "https://ethereum.org/".
[136] CORAS, "http://coras.sourceforge.net/".
[137] OLISTIC, "www.olistic.io".
[138] S. APACHE, "https://spark.apache.org/".
[139] J. S. Boot, " https://spring.io/projects/spring-boot".
[140] "State of the Industry:Cyber Risk & Captives, Spring Consulting Group," 2017. [Online]. Available: https://www.captive.com/docs/default-source/sponsor-documents/cyber-survey_captive-owners_white-paper.pdf?sfvrsn=8. [Accessed 2019].
[141] Elastic, “https://www.elastic.co/what-is/elk-stack”.
[142] Home Depot has $105 million in cyber insurance to cover data breach, https://www.businessinsurance.com/article/00010101/NEWS06/309149975/Home-Depot-has-$105-million-in-cyber-insurance-to-cover-data-breach
[143] What Does Cyberinsurance Actually Cover? https://slate.com/technology/2018/07/cyberinsurance-company-refuses-to-pay-out-full-amount-to-bank-after-hacking.html
[144] Capital One’s Data Breach Could Cost the Company up to $500 Million, https://fortune.com/2019/07/31/capital-one-data-breach-2019-paige-thompson-settlement/
[145] Around 100 Dentist Offices Affected by Sodinokibi Ransomware, https://www.cisomag.com/around-100-dentist-offices-affected-by-sodinokibi-ransomware/
[146] CYBER RISK FOR INSURERS– CHALLENGES AND OPPORTUNITIES - EIOPA https://eiopa.europa.eu/Publications/Reports/EIOPA_Cyber%20risk%20for%20insurers_Sept2019.pdf
[147] PHISH & SHIPS Issue #36 - November 2019
[148] STATE OF CYBERSECURITY: 2019 - ISACA
[149] PHISH & SHIPS Issue #34 - September 2019
[150] Kshetri, N. (2018). The Economics of Cyber-Insurance. IT Professional, 20(6), 9-14.