SECONDO: A Platform for Cybersecurity Investments and Cyber Insurance Decisions

Aristeidis Farao[1], Sakshyam Panda[2], Sofia Anna Menesidou[3], Entso Veliou[3], Nikolaos Episkopos[4], George Kalatzantonakis[5], Farnaz Mohammadi[1], Nikolaos Georgopoulos[6], Michael Sirivianos[7], Nikos Salamanos[7], Spyros Loizou[7], Michalis Pingos[7], John Polley[1], Andrew Fielder[8], Emmanouil Panaousis[9], and Christos Xenakis[1]

[1] University of Piraeus, Greece
{arisfarao, xenakis, farnaz}@unipi.gr
[2] University of Surrey, United Kingdom
[3] Ubitech Limited, Cyprus
[4] Fogus Innovations & Services, Greece
[5] Lstech Espana SL, Spain
[6] Cromar Insurance Brokers Ltd, Greece
[7] Cyprus University of Technology, Cyprus
[8] Imperial College London, United Kingdom
[9] University of Greenwich, United Kingdom

Abstract. This paper represents the SECONDO framework to assist organizations with decisions related to cybersecurity investments and cyber-insurance. The platform supports cybersecurity and cyber-insurance decisions by implementing and integrating a number of software components. SECONDO operates in three distinct phases: (i) cyber-physical risk assessment and continuous monitoring; (ii) investment-driven optimized cyber-physical risk control; and (iii) blockchain-enabled cyber-insurance contract preparation and maintenance. Insurers can leverage SECONDO functionalities to actively participate in the management of cyber-physical risks of a shipping company to reduce their insured risk.

1 Introduction

The SECONDO project addresses the question "How can we support decisions about cybersecurity investments and cyber-insurance pricing?" This is a crucial research problem as the rapid growth of cyber-attacks is expected to continue its upwards trajectory, causing fear to organizations due to potentially incurred losses: (i) *direct* losses by having their confidentiality, integrity and/or availability being compromised; or (ii) *indirect*, by having to pay vast fines as defined by the General Data Protection Regulation (GDPR). Hence, the growth of cyber-attacks presents a prominent threat to normal business operations and the EU society itself. In addition, a noteworthy finding is that an organization's computer systems may be less secure than a competitor's, despite having spent more money in securing them [1]. Obviously, in the face of uncertainties, cybersecurity investment choices and cyber-insurance, are highly challenging tasks with

serious business implications. SECONDO aims to impact the operation of EU businesses which often: (i) have a limited cybersecurity budget; and (ii) ignore the importance of cyber-insurance.

1.1 Motivation

Technological inventions and developments have started to become an integral part of any company's lifecycle. However, despite conferring significant advantages, they bring with them an enhanced cyber-physical risk of cyber incidents, and a subsequent growth in products and services aimed at combating the cyber-physical risks. In turn, the proposed solutions (products or services) come with a cost making cybersecurity investment which is a key problem for Chief Information Security Officers to tackle.

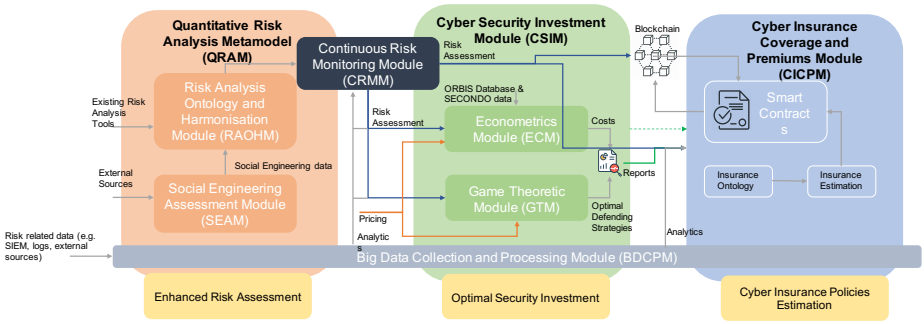
Importantly, the GDPR brings into force strengthened requirements for organizations, which process or store data as to build data protection and privacy into their organization and design, to notify the authorities of all data breaches that put individuals at cyber-physical risk. With high fines for GDPR violations (up to 20€ million or 4% of annual turnover), cyber-crime can no longer be considered an acceptable running cost of business. It provides a major impetus for organizations to proceed with optimal investments in cybersecurity solutions and procedures to minimize their cyber-physical risk exposure while transferring the residual cyber-physical risk to cyber-insurance.

1.2 Limitations

Considering the limitations discussed in [2] together with the importance of complying with GDPR and the rapid growth of cyber threats, there is an irrefutable need for developing new and automated tools to better explain and appropriately address existing and rising challenges not only through technical approaches, but also through the lens of economic analysis. Driven by market needs, SECONDO therefore proposes a unique, scalable, highly interoperable Economics-of- Security-as-a-Service platform that encompasses a comprehensive cost-driven methodology for: (i) estimating cyber-physical risks assessment 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 cyber-physical risk management by recommending optimal investments in cybersecurity controls; and (iii) determining the residual cyber-physical risks as well as estimating the cyber-insurance premiums taking into account the insurer's business strategy, while eliminating the information asymmetry between the insured and insurer. Inspired by the above functionalities and our previous work [1,3,4,5,6], we will develop the SECONDO platform to establish a new paradigm in risk management for enterprises of various sizes, with respect to the GDPR framework, while it will enable formal and verifiable methodologies for insurers that require estimating premiums.

The rest of the paper is organized as follows: Section 2 presents the SECONDO architecture and its components, whereas Section 3 describes a use case from the maritime sector and how SECONDO can be applied. Section 4 concludes the paper.

Fig. 1: Architectural components and integrated modules for SECONDO



2 SECONDO Architecture and Components

In this section, we present the SECONDO architecture (see Fig 1) along with its components and modules.

2.1 Quantitative risk assessment and data analytics

Information security management must start with a risk analysis [7]. The goal of SECONDO risks assessment is to identify: (i) relevant *threats* targeting the assets of an organization; (ii) *vulnerabilities*, both internal and external that these assets exhibit; (iii) *value-at-risk* of the organization that is equivalent to the value of assets (both tangible and intangible) being endangered by adversaries; and (iv) the likelihood that an attack will be launched against the assets. The risk represents the expected losses of an organization should one or more attacks compromise the asset affecting the confidentiality, integrity and availability of business critical services.

Asset pricing - The SECONDO platform will adopt a combination of methods for pricing *tangible* and *intangible* digital assets from a cybersecurity perspective. The objective is to provide precise point estimates on valuations of assets considering both the tangible and intangible aspects such that they can be used to directly value insurance claims in a standard actuary framework.

The outcome of the valuation methods will contribute to the Econometrics Module (ECM) which provides estimates on all kinds of costs of potential attacks.

Risk modeling - Utilizing a Quantitative Risk Analysis Metamodel (QRAM), SECONDO determine quantitative estimates of the exposed risk of an organization. It achieves this by defining methodologies for asset identification and valuation, and utilizing security metrics to quantitatively estimate risk exposure of an organization. QRAM is composed of two modules. The first, Social Engineering Assessment Module (SEAM) which is used to experimentally determine the likelihood of being exploited by social engineering attacks on different employee roles of an organization. Table 1 illustrates the results from our experimental study. The second, Risk Analysis Ontology and Harmonization Module (RAOHM) communicates with SEAM and existing risk analysis tools such as OLISTIC[1] to gather their output and harmonize through its unique vocabu-

[1] http://www.olistic.io/.

Table 1: Overall Likelihood results

Actions	**Contributor**	**Management**	**Upper Management**	**Executives**
Report Email	0	0	0	0
Email Opened	0.33	0.2	0.25	0.33
Email Sent	0.11	0	0.38	0.33
Link Clicked	0.11	0.3	0	0
Submitted Data	0.44	0.5	0.38	0.33
Attack Likelihood	0.55	0.8	0.38	0.33

lary. It uses entity-relationship diagrams between threats, vulnerabilities, security controls, assets, and identified risks with an aim to identify assets to be used in the risk analysis process. Moreover, utilizing the risk analysis ontology will assist in gathering the heterogeneous information from all business areas to support the decisions of an organization regarding its cyber governance strategy. Currently, SECONDO is implementing this module.

Big data collection and Processing Module (BDCPM) - This module of SECONDO acquires risk related data either from internal organizational sources such as network infrastructure, Security Information and Event Management, log files, users' interactions, or external sources such as social media and other internet-based sources including Darknet with specialized crawlers. This module is yet to be implemented in the project.

The collected and processed data would be specified and quantified within a meta-model, and utilizing set of data mining and learning algorithms to perform sophisticated analysis.

2.2 Cyber Security Investments and Blockchain

This segment of SECONDO will build up on the above discussed modules to compute optimal cybersecurity investment strategies and deploy blockchain technology for secure storage, access and notification of security and privacy information of organisations. This segment consists of two modules:

Continuous risk monitoring and blockchain (CRMM) - This module will continuously assess the risk levels, including the performance of the implemented cybersecurity controls.

It will update the private blockchain with information regarding the security and privacy risk of cyber-insurance clients through smart contracts. Moreover, these will notify the involved parties (insurer and insured) when the insurance terms have violated or when an event has happened to activate the insurance. These are embedded in the distributed ledger and cannot be modified due to its immutability feature providing verifiable records.

Decision-making for cyber investments - Security investment decisions with a limited budget is always a challenging task, even more in the presence of uncertainty, with massive business implications. There have been several studies [8] proposing cost-benefit approaches for selecting an optimal set of controls against cyber attacks. Along this line of work, the Cyber Security Investment

Module (CSIM) aims at computing optimal cybersecurity investment plans utilizing the Econometrics Module (ECM) and the Game Theoretic Module (GTM). ECM will provide estimates about the costs of potential attacks as well as the costs of each possible security control using a set of existing econometric models. Utilizing the asset pricing method (detailed in the previous section), ECM will also determine the impact value of an asset. On the other hand, GTM will derive strategically optimal defending strategies expressed in the form of controls to be implemented by the organization. The interaction between players is modeled as a non-cooperative game in GTM where players compete against each other. Following the widely-cited work [1], the corresponding Nash Equilibria (NE), the solution of the game, for each available cybersecurity control will be computed and sent to CSIM to compute an optimal investment solution subjected to a budget while considering the financial cost of each NE.

2.3 Cyber Insurance and Smart Contracts

The core component of this segment is the *Cyber Insurance Coverage and Premiums Module* (CICPM). This module will provide insurance exposure assessment and estimates for insurance coverage and premiums based on the insurance policies of the underlying insurer. The insurance policies will be modeled using a common vocabulary and language of cyber-insurance policies by utilizing a cyber-insurance ontology. The ontology will empower the SECONDO platform to automatically incorporate policies. Moreover, the ontology will be based on a comprehensive survey and analysis of the cyber-insurance market and well-known insurance policies as discussed in [9,10,11,12].

CICPM will not only enable underwriters to incorporate their own strategy, as required by a competitive market, but also aim at minimizing the information asymmetry between insurer and insured by applying a verifiable and shared methodology that includes standard and enhanced procedures such as quantitative risk analysis using security metrics and optimal security investments for managing cyber-physical risk. In reconciliation with CRMM, CICPM will monitor conditions leading to non-compliance of the cyber-insurance contract agreements and assist with resolving claim disputes.

3 Use case: Cyber-physical Risk Transfer in Maritime

The Maritime Cyber Risk Management guidelines [13] highlights the importance of cybersecurity technologies in facilitating critical business functions and secure operation of the maritime industry. Regardless of the increasing cyber incidents, there has been no holistic approach to manage maritime cyber-risks [14]. Further, security procedures and policies are still being defined and determined to be practiced in maritime which further results to an increasing dependency on the insurance industry.

On the other hand, the insurance industry has particularly investigated the *affirmative risks* and *silent* cyber-physical risk [15] to facilitate suitable coverage. With regards to the affirmative cyber-physical risk, the Insurance Property and

Casualty Policy [16] states that the insurer shall cover the costs of impact, either physical or digital, in case of data breach and/or network failure or attack.

Coverage capacity, cyber-physical risk estimation and appropriate solutions are difficult for insurers to manage, leading to a margin of the so called silent (unintended) cyber coverage. In this section, we summarize the applicability of the SECONDO platform in the maritime sector to achieve optimal cyber-insurance premium acknowledging both the insured's and insurer's perspective. In the recent past, physical attacks, such as piracy, was a common threat to the maritime sector.

3.1 Cyber-insurance in maritime

After the adoption of electronic systems such as sonar and IoT systems in both onshore and on-board environments, new cyber and cyber-physical vulnerabilities have emerged increasing the threat exposure of the sector. According to Alliance[2] more than 1,000 vessels have been hacked in the last five years. However, cyber losses quite often are excluded from an insurance coverage as the expected impact of cyber attacks may be considered too uncertain to be included in policy terms. Damages caused by cyber attacks or errors (e.g., damage to the vessel due to navigation system malfunctioning after being hacked) are not covered by non-cyber-insurance policies, due to a specific cyber attack exclusion clause ([10/11/2003] also known as Cl.380). According to this clause, insurers do not cover for damages caused by a cyber attack whether it includes physical harm, business interruption or property damage. Other exceptions may include terrorism-related attacks and the NMA2914 electronic data exclusion[3] creating a "cyber-insurance gap" which becomes an impediment for the maritime sector given the drastic increase of cyber incidents [17].

Although cybersecurity incidents in the maritime field increase, only few are being reported. Only major cyber attacks are made public and well-documented, such as the Maersk attack in 2017[4]. The lack of data regarding cyber attacks in maritime creates a "false sense of security" to maritime companies, making them to underestimate the expected cyber-physical risk inflicted by cyber attacks.

3.2 SECONDO Application

In this use case, we present the applicability of SECONDO in assisting a shipping company to effectively transfer its *cyber-physical risks* to an insurer provider. The risk transfer process is detailed in three different phases: (1) Cyber-physical Risk assessment; (2) Cyber-physical Risk management; and (3) Insurance exposure estimation, coverage and premium calculation.

Phase 1: The critical assets of a shipping company, as identified in [13], are vulnerable to cyber attacks inflicting cyber-physical impact and endangering the

[2] https://maritimecyberadvisors.com/_files/200000086-a389ca4859/MaritimeCyberInsurnace052019.pdf

[3] https://www.lmalloyds.com/LMA/Wordings/NMA2914A_C.aspx.

[4] https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/.

company's financial situation, reputation, property, crew's life, and the environment. This phase deals with undertake the cyber-physical risk assessment on a vessel's infrastructure and systems. It will utilize the CORAS language[5] to formalize threat models and cyber-physical risk scenarios. It will further involve in identifying assets, vulnerabilities and threats to compute the overall risk scores using the RAOHM (refer to section 2).

The output will be a quantitative estimation of the cyber-physical risks of the shipping company's infrastructure, assuming known cyber and cyber-physical maritime threats.

Phase 2: This phase deals with the cyber-physical risk management utilizing the risk assessment results from Phase 1 and data gathered by BDCPM (refer to section 2). The payoff functions and the optimal controls selection strategies are determined using the GTM and ECM (refer to section 2).

The defending strategies will reveal a mapping between the Critical Internet Security (CIS) controls[6] and various threats of the shipping company. For each CIS control, a game will be defined and solved to obtain an optimal solution. The solution of each game will determine the optimal distribution of control implementation levels (Low, Medium, High) over all targets of this use case. The payoff functions will capture both the reduction of cyber-physical risk and the indirect costs of implementing each of the controls.

CSIM (refer to section 2) will use the results of all these modules to derive optimal ways to invest in cybersecurity controls.

At the end, a smart contract will be set up between the insurance provider and the shipping company indicating the premium as well as the coverage derived from the optimal strategy.

Phase 3: In this phase, CICPM (refer to section 2) will be used to collect the results of the aforementioned modules to produce an optimal insurance premium and coverage protection. After the premium is set by the insurer, the broker communicates with the shipping company in order to analyze the contract. Along with the proposed contract terms, the shipping company must demonstrate its compliance with various information security guidelines such as BIMCO cybersecurity guidelines[7], the International Maritime Organization's Resolution on IT and OT systems [13], best practices and cyber-physical risk management, and ISO cybersecurity standards compliance. If the shipping company accepts the contract and exhibits compliance to industry and governance guidelines, then all three main actors (the shipping company, the broker and the insurer) strike an optimal deal with policies of the agreement being stored as a smart contract on a blockchain. During the smart contract lifetime, CRMM (refer to section 2) is used to continuously monitor for possible violation of the agreed policies and to convey any discrepancies on behalf of the insurance provider and the insured shipping company.

[5] http://coras.sourceforge.net/coras_language.html.

[6] https://www.cisecurity.org/controls/

[7] https://iumi.com/news/news/bimco-the-guidelines-on-cyber-security-onboard-ships.

3.3 Attack scenario

In this section, we illustrate a cyber attack scenario illustrating the usefulness of SECONDO platform in effective post-incident management.

Malware infection -

Let's assuming that the shipping company is under attack by a ransomware called CryptoMarine.

Its payload encrypted the files of all hard disks and the back-up files. Moreover, the collected data from the sensors about tank levels, nitrogen oxide concentration, temperature, and other on-board parameters [18] are encrypted. Without these values, it is extremly challenging to detect potential failures which could lead to catastrophic accidents. Further, the navigation system and telecommunications including network communications have collapsed, not permitting the vessel to successfully communicate with the onshore infrastructure of the company. As a result, this attack affects the shipping company in several different ways, since its property, crew, and reputation are jeopardized, and its share price is in a downward trend while the attackers demand ransom in cryptocurrency to unlock the encrypted devices.

Company's response team - When an employee of the shipping company identifies the incident -the ransomware infection- and, according to the shipping company's *disaster recovery policy*, the responsible officers, e.g., the Cyber Security Operation Team, as well as the Insurance Company are contacted immediately. At the same time, the *business continuity plan* is activated. The Emergency Response Team is called to action, which then assembles: (i) a Disaster Recovery Team (DRT), which is responsible for key services restoration and business continuity; (ii) a Business Recovery Team (BRT) consisting of senior members of the main departments and the management team, who are responsible for the company's operation's prompt recovery; and (iii) a Media Team, to be in contact with the media.

Insurer's role - Besides, the insurer closely cooperating with the shipping company ensuring that immediate incident response actions are taken, the recovery plan has been initiated, and a dedicated team has been assign to assist the company with the cyber defense efforts. In parallel, Personal Relations assistance is also deployed to manage the communication with the shipping company's clients that have either been affected by the attack or information regarding them has been compromised in order to be compliant with regulations such as GDPR.

Response actions - According to the Insurance Company's approach, paying the ransomware is the last option, given that alternative approaches have been planned beforehand. DRT and BRT, in collaboration with insurer's experts will work on the systems' restoration and attempt to disinfect them. First, the existing recovery plan must be applied. Existing back-up countermeasures, adopted by the shipping company prior to the incident (suggested by SECONDO), will be implemented to countermeasure the impact.

Smart contract updates - Since there is an active incident, the insurance provider initiates an immediate forensic investigation. The results of the investigation are input to the SECONDO smart contract, which automatically initiates

its process to assess the damage and decide which actions will be executed. The actions will be recommended by cross-evaluating the security practices and postures recorded by CRMM and the insurance policies.

4 Conclusion and future work

In this paper, we present the SECONDO framework that can assist organizations with decisions related to cybersecurity investments and cyber-insurance. We present the architecture of the framework and its various components. In particular, we detail how SECONDO quantitative risk assessment effective risk management optimal cybersecurity investment strategies subjected to a budget constraint. Upon successful contract agreement, SECONDO facilitates smart contracts on a blockchain which could be used for transparency, monitoring and to verify compliance to agreed insurance policies in cases of discrepancies. At last, this paper presents an overview on SECONDO's applicability in a Maritime scenario. We envisage that the implementation of SECONDO will be a significant step towards standardization of a holistic cyber economics framework for organizations of any size and sector.

Acknowledgment

This research has been funded by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie SECONDO grant agreement No 823997.

References

1. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F.: Decision support approaches for cyber security investment. Decision Support Systems **86** (2016) 13–23
2. Panou, A., Ntantogian, C., Xenakis, C.: RiSKi: A framework for modeling cyber threats to estimate risk for data breach insurance. In: Proceedings of the 21st Pan-Hellenic Conference on Informatics. (2017) 1–6
3. Fielder, A., König, S., Panaousis, E., Schauer, S., Rass, S.: Risk assessment uncertainties in cybersecurity investments. Games **9**(2) (2018) 34
4. Chronopoulos, M., Panaousis, E., Grossklags, J.: An options approach to cybersecurity investment. IEEE Access **6** (2017) 12175–12186
5. Panda, S., Panaousis, E., Loukas, G., Laoudias, C.: Optimizing investments in cyber hygiene for protecting healthcare users. From Lambda Calculus to Cybersecurity Through Program Analysis
6. Laszka, A., Panaousis, E., Grossklags, J.: Cyber-insurance as a signaling game: Self-reporting and external security audits. In: Gamesec, Springer (2018) 508–520
7. Oppliger, R.: Quantitative risk analysis in information security management: a modern fairy tale. IEEE Security & Privacy **13**(6) (2015) 18–21
8. Nespoli, P., Papamartzivanos, D., Mármol, F.G., Kambourakis, G.: Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks. IEEE Communications Surveys & Tutorials **20**(2) (2017) 1361–1396

9. Böhme, R., Schwartz, G., et al.: Modeling cyber-insurance: Towards a unifying framework. In: WEIS. (2010)
10. Woods, D., Agrafiotis, I., Nurse, J.R., Creese, S.: Mapping the coverage of security controls in cyber insurance proposal forms. Journal of Internet Services and Applications **8**(1) (2017)
11. Marotta, A., Martinelli, F., Nanni, S., Orlando, A., Yautsiukhin, A.: Cyber-insurance survey. Computer Science Review **24** (2017) 35–61
12. Romanosky, S., Ablon, L., Kuehn, A., Jones, T.: Content analysis of cyber insurance policies: how do carriers price cyber risk? Journal of Cybersecurity **5**(1) (2019)
13. Organization, I.M.: Guidelines on maritime cyber risk manageme. http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Default.aspx
14. Cimpean, D., Meire, J., Bouckaert, V., Vande Casteele, S., Pelle, A., Hellebooge, L.: Analysis of cyber security aspects in the maritime sector. (2011)
15. EIOPA: Cyber risk for insurers– challenges and opportunities. https://eiopa.europa.eu/Publications/Reports/EIOPA_Cyber%20risk%20for%20insurers_Sept2019.pdf
16. balance small business, T.: What does a cyber liability policy cover? https://www.becyberawareatsea.com/awareness
17. SANS: Bridging the insurance/infosec gap: The sans 2016 cyber insurance survey. https://www.advisenltd.com/2016/06/21/bridging-the-insuranceinfosec-gap-the-sans-2016-cyber-insurance-survey/
18. Mrakovic, I., Vojinović, R.: Maritime cyber security analysis – how to reduce threats? Transactions on Maritime Science **8** (04 2019) 132–139