SEConomy: a Framework for the Economic Assessment of Cybersecurity

Bruno Rodrigues, Muriel Franco, Geetha Parangi and Burkhard Stiller

Communication Systems Group CSG, Department of Informatics IfI
University of Zurich UZH, Binzmühlestrasse 14, CH-8050 Zürich, Switzerland
E-mail: [rodrigues,franco,parangi,stiller]@ifi.uzh.ch

Abstract. Cybersecurity concerns are one of the significant side effects of an increasingly interconnected world, which inevitably put economic factors into perspective, either directly or indirectly. In this context, it is imperative to understand the significant dependencies between complex and distributed systems (*e.g.*, supply-chain), as well as security and safety risks associated with each actor. This paper proposes SEConomy, a strictly step-based framework to measure economic impact of cybersecurity activities in a distributed ecosystem with several actors. Through the mapping of actors, responsibilities, inter-dependencies, and risks, it is possible to develop specific economic models, which can provide in a combined manner an accurate picture of cybersecurity economic impacts.

Keywords: Cybersecurity · Threats · Economics · Assessment

1 Introduction

The technological evolution and the rapid growth of the Internet have built a digital networked society, which today is an indispensable tool for communication and interaction on a planetary scale. As the number of devices (stationary or portable) increases, the complexity of systems that provide content or communication infrastructure also increases, especially to support the growing volume of traffic. As a result, these complex distributed systems are subject not only to several types of failures, but also to different types of cyber threats that can compromise CIA (Confidentiality, Integrity and Availability) aspects impairing, for example, entire societies whose Critical National Infrastructures (CNI) are connected to the Internet [8, 14].

It is imperative to understand the economics behind cybersecurity activities. For example, the United States of America (U.S.A.) released in 2018 an estimate of costs related to malicious cyber activities of around 57 and 109 billion USD for incidents appearing only in 2016 [27]. These numbers involve not only losses at the initial target and economically linked firms derived from attacks, but also incurs in costs involving the maintenance and improvement of systems security. Further, Gartner [16] corroborates with the U.S.A. estimate, predicting in 2018 a cost of 114 and 124 billion USD in 2019, representing an increase of 8% for one country only. While cost numbers are not precise on a global scale, there exist

estimates, such as [18], that predict costs related to cybersecurity activities to exceed 1 trillion USD cumulatively for the five years from 2017-2021, taking into account the growing number of Internet of Things (IoT) devices.

Systems often fail because organizations do not take into account the full costs of failure, which includes two critical categories: security (prevention of malicious activities) and safety (prevention of accidents or faults) [17]. Further, system failures often leads to business being offline (*i.e.*, security is when a conscious attack is part of the game while safety is when something fails by itself). Security investments are typically complex, because malicious activities typically expose externalities as a result of underinvestment in cybersecurity, *i.e.*, they usually exploit vulnerabilities unforeseen in the design space. Safety, however, originates from requirements, which take systems failures due to unexpected events (*i.e.,* natural disaster and/or human failures) into account to prevent the loss of lives.

In a scenario where major actors desire to minimize costs while maximizing security and safety aspects [17, 21], it is essential to understand all key cybersecurity risks, impacts, and mitigation measures (or the lack thereof) within an individually determined ecosystem economy [2]. Further, it is necessary to gain insight, into the uncertainty behind security investments. This paper contributes to the field of cybersecurity modeling with a framework allowing for an approximation of estimates and enabling the economic analysis of a given ecosystem's dimension concerning responsibilities and roles, while mapping systems and processes and their correlations as well as related costs. Thus, it is expected an understanding in detail how the economy is affected by cyber (in)security.

This paper is organized as follows. Section 2 provides the background, and related work providing an overview of how cybersecurity risks and threats are mapped into economics. Section 3 presents the Cybersecurity Economy Assessment framework and its stages, followed by a discussion and future work in Section 4.

2 Background and Related Work

Although reasons behind cyber attacks can be widely diverse, ranging from identity phishing and information security breaches to the exploiting of vulnerabilities on Critical National Infrastructures (CNI), it is notorious that these attacks have become increasingly driven by financial motives. Thus, related work focus on models analyzing economic aspects behind cyber attacks. For this reason, the U.S. Department of Defense (DoD) declares the cyberspace as the fifth dimension of defense areas, complementing the traditional land, water, sea, air warfare dimensions [15].

2.1 Cybersecurity Economics

A purely economic analysis was released in 2018 by the U.S. White House [27] revealing estimates of economic impacts in the year of 2016 (*cf.* Section 1), the

year in which one of the largest Distributed Denial-of-Service (DDoS) attack was launched on the content provider Dyn-DNS, which interrupted the delivery of content for significant Internet services (such as Twitter, PayPal, and Spotify) for a few hours. These numbers corroborate with the influence of cyber attacks in the economy (whether it is a nation or large private organizations).

[10] presented one of the fundamental models aiming to determine an optimal cost/benefit relation to cybersecurity investments. The Gordon Loeb (GL) model is intended for investments related to various information security goals (in terms of Confidentiality, Integrity, and Availability - CIA). However, although the GL model is considered a baseline for cost optimization in the cybersecurity, it is not able to handle dynamic ecosystems, *i.e.,* mapping decisions and outcomes in a single period, and not considering the time factor.

[4] builds upon [10] providing a systematic analysis on how to compare existing security investment models and metrics. While [10] defined a general security probabilistic function, the high abstraction level of its model neglects the different security levels discussed by Böhme. In this sense, [4] offers a guideline toward building an economics assessment through its systematic approach decomposing costs of security into security levels and further associating with its benefits.

[24] describes one of the approaches cited by [4], the Return Over Security Investments (ROSI). This work offers a benchmark method to evaluate the cost/benefit relation of security investments, as well as how to obtain/measure security values used in their method. However, the authors state that it is very difficult to obtain data about the true cost of a security incident once companies often do not disclose data about security breaches or vulnerabilities. Nonetheless, similarly to [10], the work does not deepen in detail the complexities of calculating security investments/expenses.

Concerning the large degree of uncertainty in security investments, the fuzzy logic becomes the appropriate method to support the decision-making process [4]. Thus, the [25] fuzzy method translates non-linear local state spaces into linear models, *i.e.,* helping to define security cost classes in which threats can be classified and translated in a cost described by a function. Thus, modeling based on ROSI [24] and a fuzzy mapping [25, 26] will be able to deal with uncertainties of security investments.

[17] discusses under economic directions impacts of cyber attacks in a national context. He bases the analysis of attacks on CNIs that could harm or collapse its economy. Also, [17] puts those principles into perspective, which motivate these attacks and policy options to prevent or respond to attacks. Thus, he proposes regulatory options to overcome barriers in cybersecurity, such as safety regulation, post liability, and others. According to the knowledge of the authors, economically-driven frameworks for a suitable and detailed assessment are not yet in place.

2.2 Mapping of Risks and Threats

The AFCEA[1] presented a discussion on cybersecurity economics in a practical framework [1]. The framework guides private organizations and the U.S. government highlighting principles to guide investments mapping risks their associated economic impacts. Threats are categorized according to its complexity *i.e.,* sophisticated or not, and its mission criticality *i.e.,* define how specific vulnerability could impair a service/process.

Concerning the mapping of risks and threats (without a direct analysis of economic impacts), the National Institute for Standards and Technology (NIST) developed a model for guiding the investment in cybersecurity countermeasures. Specifically, NIST's Special Publication 800-37 [20] and 800-53 [19] define the Cybersecurity Risk Management Framework (RMF) including a method for assessing the implementation of controls to mitigate risk. Although 800-37 and 800-53 do not present an analysis directly related to economic aspects, the NIST framework to classify risks, as well as the AFCEA mapping of risks, allows for the establishment of economic models based on threats. Although 800-37 and 800-53 do not present an analysis directly related to economic aspects, the NIST framework (as well as the AFCEA) to classify risks, allows for the establishment of economic models based on threats.

Also, specific guides/frameworks exists for the different cyber systems and applications. For example, while NIST guides focus on the overall risks of an organization, STRIDE [9], LINDDUN [28], or DREAD [23], map each specific type of threat as well as their mitigation actions. For instance, STRIDE (Spoofing, Tampering, Repudiation, Information (disclosure), Denial-of-Service, and Elevation of Privilege) is an industrial-level methodology that comes bundled with a catalog of security threat tree patterns that can be readily instantiated [9]. DREAD is a mnemonic (Damage potential, Reproducibility, Exploitability, Affected users, Discoverability), which, although similar, represents a different approach for assessing threats [23]. LINDDUN builds upon STRIDE to provide a comprehensive privacy threat modeling [28].

Aiming at the evaluation of economic risks, [21] proposes a proactive model to simulate economic risks of CNI's with integrated operations, *i.e.,*, that links many vendors, suppliers into the same ecosystem. The authors seek to map inter-dependencies amongst actors to establish a causal relation, which can then be used to estimate economic risk under various scenarios. However, despite providing a view on the inter-dependencies between the actors, the proposed model does not consider problems that may later occur because of a rush to attain initial economic gains.

For an effective mapping of factors influencing the safety and security of an ecosystem, it is necessary to have an accurate idea of its threats, and risks. SEConomy relies on these mappings, which, for example, can be guided by the frameworks described. Further, it is necessary to understand the interdependence between systems/subsystems, which can trigger cascade failures.

[1] Non-profit organization serving military, government, industry, and academia.

3 SEConomy Framework

In ecosystems involving different actors ensuring certain security/safety levels is not a straightforward task. Due to the number of participants potentially managing sensitive information or critical tasks, the risk assessment of a supply chain, for example, becomes complicated [2, 7]. The framework proposed (*cf.* Figure 1) takes into consideration the economic analysis of complex systems by structuring to five stages of mapping and modeling, allowing the creation of economic models with fine-grained estimates.

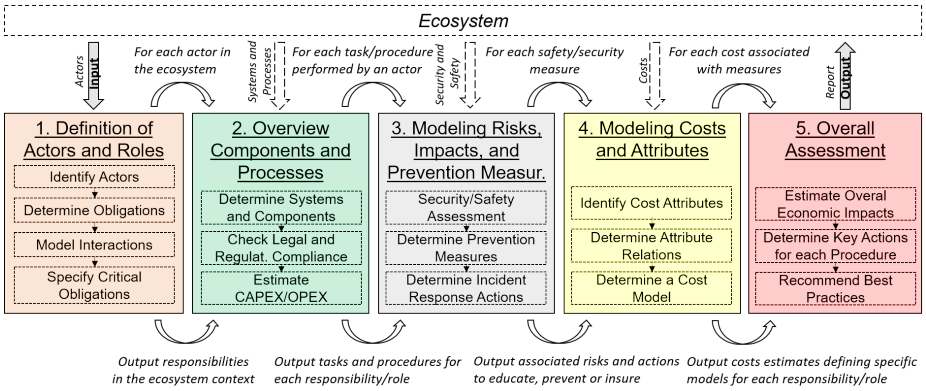

Fig. 1. SEConomy Framework

Stage 1 is concerned with the definition of actors and their functions, whose interactions should be mapped as well as which critical functions should be specified. Stage 2 to determines which systems/components and processes are performed by these actors and their legal implications for an initial attribution of investment and operating costs. Based on the mapping of actors, systems, and processes, Stage 3 is responsible for the production of risk models and possible impacts as well as preventive and training measures based, for example, on NIST risk assessment guides 800-37 and 800-53 [20, 19]. Stage 4 takes into consideration this risk analysis to map costs in a fine-grained manner, *i.e.*, for each risk of each task performed by each actor previously mapped. Lastly, Stage 5 gathers outputs of Stage 4 to a produce general feedback in terms of overall economic impacts, the determination of improvement actions, and best practices.

3.1 Definition of Actors and Roles

It is possible to consider as input, for example, the production chain of an aircraft system as a complex ecosystem that requires an assurance of security and safety levels based on a detailed risk analysis of all its major control components. A comparative between Airbus and Boeing supply-chains [11] have shown, for

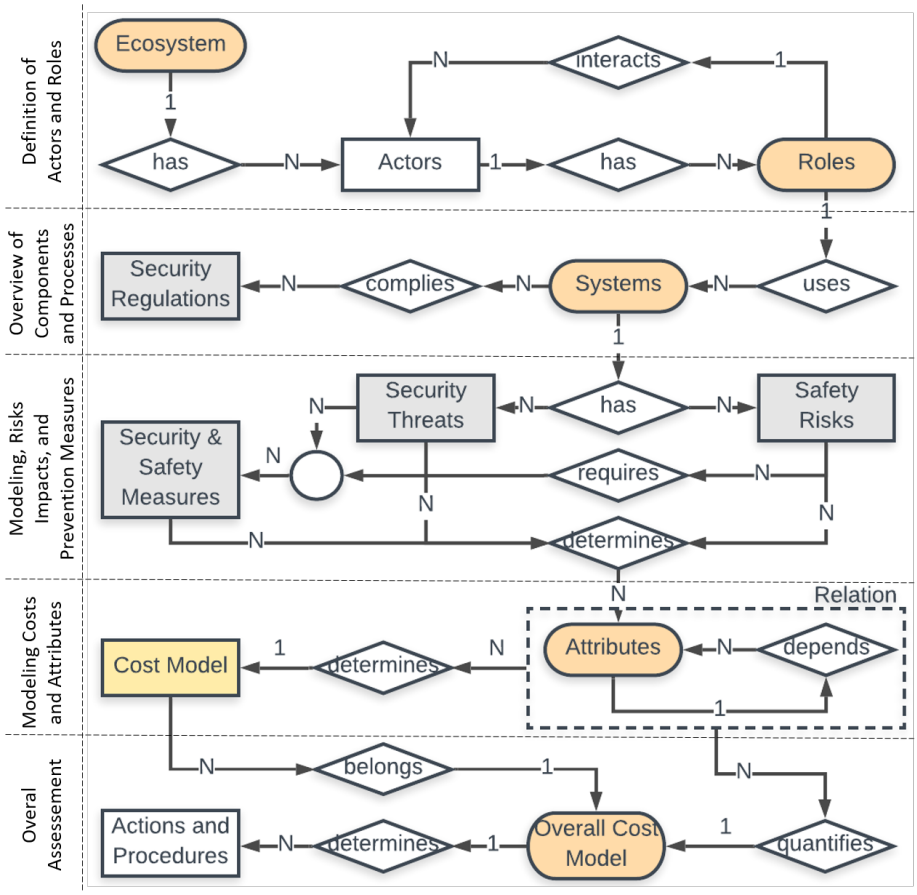

Fig. 2. SEConomy entity-relation model between stages

example, that the manufacture of the wide-body Airbus A380 and Boeing 787 aircraft involves multiple suppliers from 30 and 67 countries, respectively. Hence, it is essential in Stage 1 to identify all actors involved in the supply chain, and their roles (and determination of which tasks/functions are critical). Figure 2 shows as a first step the identification of actors involved (*e.g.,* producers of flight control systems, software for engines) as well as their obligations and interactions with other actors. In this regard, Boeing and NIST defined a guideline on cybersecurity supply-chain risk management [22], where the organizations that provide software for their aircrafts must undergo a rigorous inspection process. It should be noted, however, that even the most rigorous processes are subject to failures as recently observed in the Boeing 737 Max accident [3].

3.2 Overview of Components and Processes

Among the actors' obligations, it is necessary to identify the ones whose roles involve critical processes/systems and components. In the case of the aviation sector, these include producers of navigation and communication systems, traffic collision avoidance, and Fly-By-Wire (FBW) systems [22]. The mapping of systems and components is crucial for the analysis of risk, which involves not only technical, but also human aspects. For example, critical systems require not only a guarantee of safety and security aspects, but also whether actors operating these systems can monitor and react. Also, these systems should comply with security and safety regulations/recommendations, which measurably leads to implications of Capital or Operational Expenditures (CAPEX/OPEX). For example, the Airbus A320 FBW system uses five different computers running four flight control software packages to ensure reliability/availability [13], complying with the U.S.A. Federal Aviation Administration agency requirements for safety matters in the design of FBW systems.

3.3 Modeling Risks, Impacts, and Prevention Measures

As presented in Figure 2, each system requires an analysis of its potential security/safety threats, and measures to respond to these threats. A rational approach in defining what is "appropriate" involves (a) identification of risks by examining potential vulnerabilities and their chances of a successful exploitation, (b) the cost of these results if vulnerabilities are exploited, and (c) the cost of mitigating vulnerabilities. The risk analysis is the fundamental stage toward mapping costs associated with cybersecurity. It is responsible for determining, proactively or reactively, possible vulnerabilities/threats (*i.e.*, probabilities) that may occur as a function of time as well as their associated counter-measures.

Risk/Threat Assessment. SEConomy require as input the analysis of threats and risks, which can be based, for example, on frameworks such as the NIST 800-37/800-53 [20, 19], and different frameworks (*cf.* Section 2), such as STRIDE [9], LINDDUN [28] or DREAD [23], which provide a mapping of threats into categories and their respective mitigation measures.

Mapping Dependencies (MD). The challenge is, however, to translate in a quantifiable manner risks and associated security measures in terms of costs, which includes not only estimating the probability of a threat to be successfully exploited, but also the mapping of interdependence between failures. Correlations can be mapped as the correlation between two Bernoulli random variables (A, B) as defined in [6]:

$$MD(A,B) = p_X = \frac{p_X - p_A * p_B}{\sqrt{p_A(1-p_A) * p_B(1-p_B)}} \tag{1}$$

p_A and p_B denotes the probability of failure in a system A and B, respectively. These probabilities, as defined in [10], are described in values between $p(0 \leq p \leq$

1), representing the probability of breaches to occur under current conditions. The inter-dependence, given in Eqn. (1), denotes a failure probability p_X, where p_A may lead to a failure in p_B, *i.e.,* failures or vulnerabilities in a component (p_A) under certain conditions can compromise the related components p_B.

3.4 Modeling Costs and Attributes

This stage determines measures to be taken in response to each threat and their associated costs. For example, the ROI (Return On Investment) of proactive approaches (education/training of personnel, prevention, and redundancy of critical systems) is a better economic alternative than reactive approaches (active monitoring and recovery). However, the remaining difficulty is to efficiently determine cost thresholds for CAPEX and OPEX.

Threat Exposure Cost (TEC). The SECeconomy approach is based on the ROSI (Return On Security Investment) model that determines the cost/benefit ratio related to security strategies [24, 5]: Single threat exposure costs in Eqn. (2) estimate the total cost of vulnerabilities given their probable occurrences within a time frame $\Delta T \left(\frac{prob(N_{occurrences})}{time}\right)$:

$$TEC(A,B) = \Delta T * \left(\sum_{i=1}^{\mathrm{N}_{Threats}} ThreatCost * MD(A,B) \right) \tag{2}$$

There are two significant challenges to quantify vulnerability costs in Eqn. (2): (a) economic impacts of vulnerabilities identified ($ThreatCost$) and (b) potential impacts given by $MD(A,B)$ on the K dependent systems. However, impacts on dependencies are equally not straightforward to be estimated, because the failure of one component may not always lead to the failure of another dependent system (*e.g.,* the use of a layered defense or a "sufficient" redundancy level may reduce such risks). For example, a failure in a fuel control subsystem may not always impair an aircraft's turbine, because a redundancy level of computers exists to provide input for the FBW and, typically, more than one turbine is used in a commercial wide/narrow-body aircraft.

Proactive Mitigation Cost (PMC). These costs are mapped based on proactive and reactive measures [12]. The PMC presented in Eqn. (3) is relatively simpler than the reactive costs. This is because the risk vector is foreseen in assessment guides/frameworks, and their mitigation actions and associated PMCs are taken into account at system design time. Additionally, it is possible to include an $InsuranceCost$ that allows the recovery of unforeseen costs.

$$PMC(A) = \sum_{i=1}^{\mathrm{N}_{Threat}} \Delta T * (ProactiveCost + InsuranceCost) \tag{3}$$

Reactive Mitigation Cost (RMC). *RMC* are challenging to be estimated, since these failures or vulnerabilities are typically originated from unforeseen design aspects, implying on a *ReactiveCost* to mitigate the threat and its consequences on potentially connected systems. However, the cost of reactive mitigation do not always present a linear relation with time, *i.e.*, the longer the time to perform a reactive measure not always mean that its cost will be higher. For example, in case of a vulnerability in which an attacker gains privileged access to a private network, this does not always imply that the longer time, the higher the victim's monetary loss. However, in case of a DDoS attack, there is a temporal relation taking into account that the greater the time a content provider do not provide service, the greater will be the economic damage on the victim.

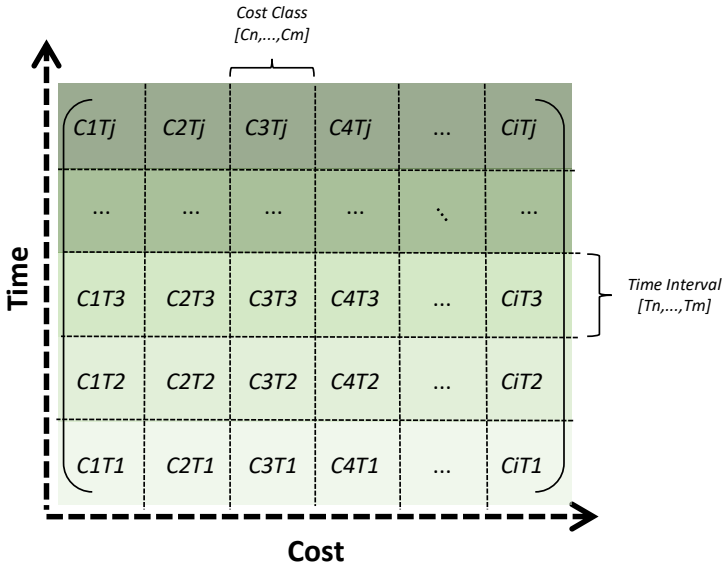

Fig. 3. MTC matrix describing time-cost classes, where C_iT_j classes represent a cost function $f(x, y)$

As described in Sec. 2, [25] proposed a type of fuzzy model, which translates local dynamics in different state space regions represented by linear models. Based on their proposal, it is defined in SEConomy different classes of RMC costs C_i in function of time T_j, whereas each class has its own cost function. Similarly to PM_{costs}, there is also the alternative to adopt an insurance model to cover potential impacts of subsystems or directly connected systems. Further, the cost of a reactive measure (and potential effects dependent systems) can be mapped in the MTC matrix (*cf.* Figure 3). On the one hand, data breaches are not time-sensitive, but may incur in high costs depending on how sensitive is the exposed information. Hence, a data breach could occur in a time $T1$ with a

cost Ci, in which i would define the relevance of the exposed information. On the other hand, a DDoS attack is time-sensitive meaning that the longer is the time without providing services (*i.e.,* higher Tj imply in higher Ci), the higher is the economic damage expressed by the time-cost category function.

In detail, a typical fuzzy rule defined by [25] is expressed by an Event-Condition-Action (ECA) rule, where the action is expressed by a function:

$$If\ x\ is\ C\ and\ y\ is\ T\ Then\ Z = f(x, y) \tag{4}$$

C and T are defined, respectively, in terms of cost and time, in which C_iT_j classes are associated with a linear cost function in the MTC matrix [26]. Cost classes are defined as $Ci = [C_n, ..., C_m]$, where n and m belongs to $\mathbb{R}_{\geq 0}$ and Time $C_z, ..., C_w$, where z and w correspond to a class time interval defined in $\mathbb{N}$. For example, a RMC that happened during a time interval "T1", can be associated, depending on the involved systems, with a cost category $C1$ defined as "low cost". Thus, a $C1T1$ is associated with a cost function of $z = F(C1, T1)$, which describes a price category. As previously mentioned, a $CiT1$ category could express, for example, a data breach. Thus, based on [25], time-cost relations can be expressed in terms classes of cost functions mapped in the MTC matrix. However, to foretell the economic impact on dependent systems, which relies on the probabilistic dependence of Eqn. (1), it is necessary to consider failures/vulnerabilities which can trigger cascading failures on correlated systems/subsystems potentially impairing the functioning of the entire system, *cf.* Eqn. (5).

$$RMC(A, B) = \sum_{i=1}^{\mathrm{N}_{System}} \left(\sum_{i=1}^{\mathrm{N}_{Threat}} \underbrace{MD(A, B)}_{\substack{\text{Probability of} \\ \text{Cascade Failures}}} * \overbrace{MTC[C_i][T_j]}^{\substack{\text{Cost Function} \\ \text{f(x,y)}}} \right) \tag{5}$$

ROSI. To benchmark the security investments is necessary to take into account initial investments in security (*i.e., PMC* proactive measures) of a system in a given time-frame ΔT (*e.g.,* monthly), multiplied by the risks, threats which the system is exposed (T_{cost}) considering its probable occurrence (RMC). Finally, Eqn. (6) calculates ROSI for a single system taking as input the threat vector (T_{cost}), mitigation costs (RMC), and initial investments in security (PMC).

$$ROSI = \Delta T * \sum_{i=1}^{\mathrm{N}_{System}} \frac{(T_{costs} * RMC) - PMC}{PMC} \tag{6}$$

3.5 Overall Economic Assessment

In the last stage, it is necessary to calculate the overall economic impact based on ROSI from all S systems, required by R roles of A actors. Therefore, as illustrated in Figure 2, the N economic models will define an overall estimate of costs for the entire ecosystem, as illustrated by Algorithm 1.

Algorithm 1: Overall Economic Assessment (OEA)

```
1 begin
2     for each Actor ∈ Ecosystem:
3         for each Role ∈ Actor:
4             for each System ∈ Role:
                  /* Correlation between linked systems in Equation 1  */
5                 p(x) ← dependence(System, ∀ linkedSystems)
                  /* Estimate exposure costs in Equation 2             */
6                 threat_costs ← T_costs(A, p(x))
                  /* Estimate mitigation (Proactive and Reactive) costs
                     in Equation 3                                     */
7                 mitigation_costs ← PMCcosts(A)
8                 mitigation_costs ← RMCcosts(A, p(x))
                  /* Get Overal Economic Assessment (OEA) in Equation 4
                     */
9                 OEA ← ROSI(threat_costs, mitigation_costs, InitSecCost)
```

4 Discussion and Future Work

The SEConomy proposes a framework to detail economic estimates for security measures in complex distributed systems. Despite providing estimates based on historical events and probabilities, failures and vulnerabilities in critical systems typically result in failures of sub-components or related systems, impacting the overall costs. Hence, it is also imperative to react on threats through reactive mitigation actions, and although its associated costs are not straightforward to be calculated, it is possible to map them into categories as proposed in the SEConomy.

For example, despite all recent technological advances, the introduction of a new warning component in the Boeing 737 Max caused two accidents with hundreds of fatalities [3]. Specialists stated that a software failure (*i.e.,* not properly implemented/tested) in the "Angle-Of-Attack (AOA)" sensors were triggering the flight control system to push the nose of the aircraft down repeatedly. In this regard, the calculation of risks through mutual vulnerability exposure along with other horizontal (*i.e.,* subsystems of a system) and vertical (*i.e.,* systems of another actor relations) is a complex task of potential security and safety consequences.

Thus, the presented SEConomy is a novel framework for estimating costs in complex distributed systems, which provide models for cost estimations and the mapping of relations between interdependent systems and their components. Thus, the need to refine these models especially for cybersecurity defense mechanisms becomes visible. Future work will run this refinement as well as the proposal of cyber-insurance models capable of covering the mitigation of threats not foreseen during design. Also, SEConomy will be applied for in-depth evaluations in different use cases such as Finance and e-Health sectors, while applying specific models from each sector for their respective economic estimates.

Acknowledgements

This paper was supported partially by (a) the University of Zürich UZH, Switzerland and (b) the European Union's Horizon 2020 Research and Innovation Program under grant agreement No. 830927, the Concordia project.

References

1. AFCE: The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment. The AFCE Cyber Committee , 2013, https://www.afcea.org/committees/cyber/documents/cybereconfinal.pdf
2. J. Bauer, M. Van Eeten: Introduction to the Economics of Cybersecurity. Communications and Strategies, **vol. 81**, pp. 13–22, 2011
3. BBC: Boeing Admits It 'Fell Short' on Safety Alert for 737. BBC News. pp. 1–3, 2019, https://www.bbc.com/news/business-48461110
4. R. Böhme: Security Metrics and Security Investment Models. In: International Workshop on Security. Springer, 2010, pp. 10–24
5. M. Brecht, T. Nowey: A Closer Look at Information Security Costs. In: The Economics of Information Security and Privacy, pp. 3–24. Springer, 2013
6. P. Y. Chen, G. Kataria, R. Krishnan: Correlated Failures, Diversification, and Information Security Risk Management. MIS quarterly pp. 397–422, 2011
7. S. Dynes, E. Goetz, M. Freeman: Cyber Security: Are Economic Incentives Adequate? In: E. Goetz, S. Shenoi (eds.) Critical Infrastructure Protection. Springer US, Boston, MA, 2008, pp. 15–27
8. M. Felici, N. Wainwright, S. Cavallini, F. Bisogni: What's New in the Economics of Cybersecurity? IEEE Security and Privacy, **vol. 14**, pp. 11–13, may 2016. https://doi.org/10.1109/MSP.2016.64
9. P. Garg, L. Kohnfelder: The Threat to Our Products. Microsoft pp. 1–8, 1999, https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx
10. L. A. Gordon, M. P. Loeb: The Economics of Information Security Investment. ACM Transactions on Information Systems Security, **vol. 5**, pp. 438–457, Nov 2002. https://doi.org/10.1145/581271.581274
11. T. C. Horng: A Comparative Analysis of Supply Chain Management Practices by Boeing and Airbus: Long-term Strategic Implications. Master Thesis, Massachusetts Institute of Technology (MIT) , 2006
12. N. Jentzsch: State-of-the-Art of the Economics of Cyber-Security and Privacy. IPACSO Deliverable D4.1, **vol. 4**, 2016
13. A. J. Kornecki, K. Hall: Approaches to Assure Safety in Fly-By-Wire Systems: Airbus vs. Boeing. In: IASTED Conf. on Software Engineering and Applications, 2004
14. L. A. Maglaras, K. H. Kim, H. Janicke, M. A. Ferrag, S. Rallis, P. Fragkou, A. Maglaras, T. J. Cruz: Cyber Security of Critical Infrastructures. ICT Express, **vol. 4**, pp. 42 – 45, 2018. https://doi.org/https://doi.org/10.1016/j.icte.2018.02.001, http://www.sciencedirect.com/science/article/pii/S2405959517303880, sI: CI and Smart Grid Cyber Security
15. C. McGuffin, P. Mitchell: On domains: Cyber and the Practice of Warfare. International Journal: Canadas Journal of Global Policy Analysis, **vol. 69**, pp. 394–412, 2014

16. S. Moore: Gartner Forecasts Worldwide Information Security Spending to Exceed 124 Billion in 2019. Gartner , 2018, https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019
17. T. Moore: The Economics of Cybersecurity: Principles and Policy Options. International Journal of Critical Infrastructure Protection (IJCNIP), **vol. 3**, pp. 103 – 117, 2010. https://doi.org/https://doi.org/10.1016/j.ijcip.2010.10.002, http://www.sciencedirect.com/science/article/pii/S1874548210000429
18. S. Morgan: 2019 Official Annual Cybercrime Report. Herjavec Group , 2019, https://bit.ly/2TouUT2
19. NIST: Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology (NIST) Special Publication, **vol. 800**, pp. 8–13, 2013
20. NIST: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Tech. rep., National Institute of Standards and Technology (NIST), 2014
21. E. Rich, J. J. Gonzalez, Y. Qian, F. O. Sveen, J. Radianti, S. Hillen: Emergent Vulnerabilities in Integrated Operations: A Proactive Simulation Study of Economic Risk. International Journal of Critical Infrastructure Protection, **vol. 2**, pp. 110 – 123, 2009. https://doi.org/https://doi.org/10.1016/j.ijcip.2009.07.002, http://www.sciencedirect.com/science/article/pii/S1874548209000183
22. S. Robert, T. Vijay, Z. Tim: Best Practices in Cyber Supply Chain Risk Management. US Resilience Project pp. pp. 1–14, 2016
23. A. Shostack: Experiences Threat Modeling at Microsoft. Microsoft pp. 1–11, 2008, https://adam.shostack.org/modsec08/Shostack-ModSec08-Experiences-Threat-Modeling-At-Microsoft.pdf
24. W. Sonnenreich, J. Albanese, B. Stout, et al.: Return On Security Investment (ROSI)- A Practical Quantitative Model. Journal of Research and practice in Information Technology, **vol. 38**, pp. 45–52, 2006
25. T. Takagi, M. Sugeno: Fuzzy Identification of Systems and its Applications to Modeling and Control. In: Readings in Fuzzy Sets for Intelligent Systems, pp. pp. 387–403. Elsevier, 1993
26. H. O. Wang, K. Tanaka, M. F. Griffin: An Approach to Fuzzy Control of Nonlinear Systems: Stability and Design Issues. IEEE Transactions on Fuzzy Systems, **vol. 4**, 14–23, 1996
27. WhiteHouse: The Cost of Malicious Cyber Activity to the U.S. Economy. White House , 2018, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
28. K. Wuyts, R. Scandariato, W. Joosen, M. Deng, B. Preneel: LINDDUN: A Privacy Threat Analysis Framework. DistriNet pp. 1–23, 2019, https://people.cs.kuleuven.be/ kim.wuyts/LINDDUN/LINDDUN.pdf