e-ISSN: 2236-0972
https://doi.org/10.5585/gep.v13i3.23083
Recebido em: 15 out. 2022
Aprovado em: 07 nov. 2022
Editor Chefe: Luciano Ferreira da Silva
Editor Científico: Flavio Santino Bizarrias
Editor Científico: Renato Penha

A FRAMEWORK FOR THE PLANNING AND MANAGEMENT OF CYBERSECURITY PROJECTS IN SMALL AND MEDIUM-SIZED ENTERPRISES

UM FRAMEWORK PARA PLANEJAMENTO E GERENCIAMENTO DE PROJETOS DE CIBERSEGURANÇA EM PEQUENAS E MÉDIAS EMPRESAS

Muriel Figueredo Franco
Ph.D.
University of Zurich – UZH – Communication Systems Group.
Zürich – Switzerland.
franco@ifi.uzh.ch

Fabricio Martins Lacerda
Ph.D.
Universidade Estadual do Paraná – UNESPAR – Centro de Ciências Sociais Aplicadas
Apucarana, Paraná – Brazil.
fabriciomlacerda@gmail.com

Burkhard Stiller
Ph.D.
University of Zurich – UZH – Communication Systems Group.
Zürich – Switzerland.
stiller@ifi.uzh.ch

Abstract
Cybersecurity remains one of the key investments for companies that want to protect their business in a digital era. Therefore, it is essential to understand the different steps required to implement an adequate cybersecurity strategy, which can be viewed as a cybersecurity project to be developed, implemented, and operated. This article proposes SECProject, a practical framework that defines and organizes the technical and economics steps required for the planning and implementation of a cost-effective cybersecurity strategy in Small and Medium-sized Enterprises (SME). As novelty, the SECProject framework allows for a guided and organized cybersecurity planning that considers both technical and economical elements needed for an adequate protection. This helps even companies without technical expertise to optimize their cybersecurity investments while reducing their business risks due to cyberattacks. In order to show the feasibility of the proposed framework, a case study was conducted within a Swiss SME from the pharma sector, highlighting the information and artifacts required for the planning and deployment of cybersecurity strategies. The results show the benefits and effectiveness of risk and cost management as a key element during the planning of cybersecurity projects using the SECProject as a guideline.

Keywords: Cybersecurity. Risk management. Cost management. Project management.

Resumo
Investimentos adequados em cibersegurança continuam sendo um dos principais pilares para empresas que necessitam proteger seus negócios em uma era digital. Para isto, é essencial compreender os diferentes passos necessários para implementar uma estratégia adequada de cibersegurança, que pode ser vista como um projeto de cibersegurança a ser desenvolvido, implementado e operado por uma empresa. Este artigo propõe o SECProject, um framework que define e organiza as etapas técnicas e econômicas necessárias para o planejamento e implementação de uma estratégia de segurança cibernética econômica em Pequenas e Médias Empresas (PMEs). Como resultado, as etapas do SECProject permitem um planejamento guiado e organizado de cibersegurança que considera tanto elementos técnicos quanto econômicos necessários para uma proteção adequada. Isto ajuda até mesmo empresas sem experiência técnica a otimizar seus investimentos em segurança cibernética enquanto reduzem seus riscos comerciais devido a ciberataques. A fim de mostrar a viabilidade do framework proposta, foi realizado um estudo de caso dentro de uma PME suíça do setor farmacêutico, destacando as informações e artefatos necessários para o planejamento e implantação de estratégias de cibersegurança. Os resultados mostram os benefícios e a eficácia da gestão de riscos e custos como um elemento-chave durante o planejamento de projetos de cibersegurança, utilizando o framework SECProject como diretriz.

Palavras-chave: Cibersegurança. Gerenciamento de riscos. Gerenciamento de custos. Gerenciamento de projetos.

Cite como
American Psychological Association (APA)

Franco, M. F., Lacerda, F. M., & Stiller, B. (2022, set./dez.). A framework for the planning and management of cybersecurity projects in small and medium-sized enterprises. *Revista de Gestão e Projetos (GeP)*, *13*(3), 10-37. https://doi.org/10.5585/gep.v13i3.23083

1 Introduction

Cyberattacks determine a rising threat for governments and companies. As businesses become more digital, they are exposed to an increasing number of threats, such as Distributed Denial-of-Service (DDoS) attacks, ransomware, and data breaches (Liu et al., 2018). Thus, beyond compromising companies' and their customers' security and privacy, malicious attackers can negatively impact the economy of businesses or services supported by digital systems.

Predictions from the Cybersecurity Ventures, the world's leading researcher for the global cyber economy, indicate that cybercrime damages will hit US$ 10 trillion (United States Dollars) annually by 2025 (Cybersecurity Ventures, 2020). Such damages include direct and indirect costs, such as those involved with the loss of critical data, asset theft, business disruption, and reputation harm (Gordon, Loeb, & Zhou, 2021). Thus, it is essential to think and plan cybersecurity not only on the technical side but also considering the economic and societal impacts of digital threats (Franco et al., 2023).

However, even with the rising of cyberattacks, there is still a wrong perception of risks and a lack of cybersecurity investments from different companies (ENISA, 2021). Today, Small and Medium-sized Enterprises (SME) are among the ones most exposed to cyberattacks. For instance, according to the results of a recent survey (Cynet, 2021), 63% of the Chief Information Security Officer (CISO) of companies think the risks are higher in small companies (less than 250 employees) than in larger ones. SMEs often fail to evaluate their risks and underestimate the impacts of cyberattacks on their businesses (European Digital Alliance SME, 2020).

As SMEs have limited budgets, they frequently think of investments in cybersecurity as an additional cost but not as an investment to avoid future financial losses due to cyberattacks or leakages. This view results in insufficient time, personnel, and money dedicated to handling cybersecurity demands. Also, there is a lack of in-house knowledge to handle the different challenges for the implementation of cybersecurity (Franco et al., 2022), which involve identifying threats, planning the investments, and managing all tasks required to conduct projects that result in an efficient cybersecurity strategy.

Thus, the steps required to analyze the requirements and costs to implement cybersecurity strategies in SMEs are critical for achieving a proper level of protection for businesses and their customers (Franco, Rodrigues, & Stiller, 2019). Therefore, different

elements have to be considered to ensure that the development of a cybersecurity project is economically (costs management) and technically (risks management) viable for SMEs.

Cybersecurity can benefit from the different models, processes, and standards already well-established in the project management field (Project Management Institute, 2017). Therefore, there are opportunities for the proposal of novel approaches (Presley & Landry, 2016) that help decision-makers consider essential elements to make the best decisions regarding cybersecurity strategies in their companies (Lee, 2021). These approaches can help to achieve a cost-effective and feasible project to be implemented for the protection of their businesses and customers. Thus, there is room for works that combines the best practices of project management and the know-how of cybersecurity economics to provide a systematic way for decision-makers to identify and understand relevant elements during the planning and execution of projects to implement cybersecurity strategies in businesses.

This article proposes the SECProject, a framework to determine steps, processes, and information to be considered during the execution of a project to implement or update cybersecurity strategies in SMEs. SECProject investigates two main research questions: (i) how to manage the costs and project risks during the implementation of cybersecurity strategies in SMEs? and (ii) how to maximize the resources (i.e., time, money, and technical expertise) in order to achieve a proper level of security for the critical processes of a business?

The proposed framework consists of six different pillars: (a) Briefing and Business Demands, which describes the most important information about the business and the past experiences with cyber threats, (b) Threat Modeling and Security Risk Analysis, which involves the process of analyzing the current cybersecurity of the business, (c) Project Requirements that determines the goals and demands to be achieved with the project, (d) Cost Management, which determines the costs of the different steps and the optimal investment in cybersecurity (e) Project Risk Management to identify and mitigate risks that leads the project to possible failures, and, finally, (f) Execution and Deployment of the project that implements the cybersecurity strategy. All of these pillars are described in details in this article.

Also, a practical case study is conducted to give evidence of the feasibility of the proposed framework. The case study comprises a hypothetical Swiss SME defined based on real-world information obtained from different report analysis, research and academic networking with an ecosystem composed of 54 universities and companies from Europe (CONCORDIA Consortium, 2022), interviews with four CEOs of Swiss SMEs working

directly with innovation, and nine risk analysts and cybersecurity insurance underwriters. The interviews and discussions are supported by different methodologies, such as those discussed by Qu & Dumay (2011) and Cairns-Lee, Lawley & Tosey (2022). Additionally, a discussion on challenges and best practices for executing cybersecurity projects in SMEs is provided.

The remainder of this article is organized as follows. Background and Related Work are presented in Section 2, while the methodology, paths investigated, and tools used during the development of this study are discussed in Section 3. The SECProject framework is introduced in the Section 3 as well as a practical case study is presented. Finally, the last section concludes the work providing the final remarks and give insights on future work and research directions.

2 Theoretical background

The role of cybersecurity is clear for companies and society in the following years (or even decades). Companies have to carefully consider all of these investments in cybersecurity, since the threats can be considerably reduced by doing correct investments and planning (*e.g.*, based on risk assessments, threats landscape, and reliable metrics). A survey sponsored by IBM Security states that cybersecurity response planning is slowly improving. However, cybersecurity in companies is becoming too complex due to the use of many different tools without sufficient knowledge (IBM Security & Ponemon Institute, 2020). At this point, it is possible to understand that the cybersecurity risks that SMEs and Multinational Enterprises (MNE) face are pretty similar. However, according to the company, some specific threats are more common (*e.g.*, data breaches are twice as common in larger companies as in smaller companies). The significant difference lies in the ability of SMEs and MNEs to handle these risks. Despite technological advantages for larger firms, both MNEs and SMEs face challenges when it comes to recruiting new cybersecurity talent, with the labor market for such experts being scarce.

Thus, both MNEs and SMEs have to consider training strategies to fill the skills gap. It has also been noted that SMEs are getting targeted more and more often by malicious actors whose goal is to enter a supply chain's information system through the weakest link. Thus, besides cybersecurity solutions, critical investments have to be made to increase cybersecurity staff and promote more cybersecurity awareness for their general employees. Also, companies have to make sure they can detect and mitigate cyberattacks effectively, with a clear cybersecurity strategy tailored for the reality of the company (*e.g.*, personnel culture, size,

sector, and budget) while covering all relevant facets of cybersecurity (e.g., detection, mitigation, and recovery plans). Besides the technical aspect of cybersecurity, the implementation of cybersecurity strategies also depends on an effective execution of projects to address all companies' requirements with an effective cost management.

Table 1 lists examples of different type of incentives to promote a better cybersecurity. An important regulation in Europe that went into force in 2018 is the General Data Protection Regulation (GDPR). The GDPR is a law for privacy and security that defines rules for every company that processes the personal data of EU citizens or residents, including companies that offer goods or services for such people. Therefore, the GDPR applies even to companies not located in the EU but that offer services there. This regulation also inspired the Brazilian General Personal Data Protection Law (LGPD – translation from the original term in Portuguese “Lei Geral de Proteção de Dados”), which empowers individuals inside Brazil with nine enforceable rights over their own personal data and make mandatory a set of best practices for companies handling data of Brazilian citizens.

Also, guidelines have been provided along the years to support cybersecurity implementation in companies. For example, the European Watch on Cybersecurity & Privacy started to provide guidance to help SMEs understand where to start implementing required standards and technical specifications. An SME, if satisfying all requirements, can receive a Cybersecurity Label as a low-cost solution that assesses and showcases its cybersecurity posture (European Watch on Cybersecurity & Privacy, 2021).

Table 1.

Examples Of Initiatives For Cybersecurity Regulations, Organizational Guidelines, And Threat Modeling Approaches

Name	Type	Main Stakeholders
Cybersecurity Label	Guideline	EU SMEs and Startups
NIST Framework	Guideline	Companies in general
GDPR	Regulation	All EU Member States
LGPD	Regulation	All Companies Handling Brazilian Data
STRIDE	Threat Modeling	Companies in general
DREAD	Threat Modeling	Companies in general
CoReTM	Methodology	Companies in general
CET	Questionnaire-based tool with 35 questions based on NIST CSF	Companies in general
Cybersecurity Canvas	Methodology	SMEs
Cybersecurity Osservatorio	Self-assessment questionnaire	SMEs
SECProject (This work)	Framework	SMEs

Source: Original data of the research.

Besides regulations, there are also well-known approaches from standardization institutes. For example, the National Institute of Standards and Technology (NIST) of the United States of America (USA) defined, with its latest version released in April 2018, a framework to guide cybersecurity activities as part of the organization's risk management processes (NIST, 2018).

Furthermore, different threat modeling methodologies are placed (Xiong & Lagerstrom, 2019). For instance, STRIDE stands as a threat model for Spoofing, Tampering, Repudiation, Information, Denial-of-Service, and Elevation of Privilege. It is an industrial-level methodology that comes bundled with a catalog of security threat tree patterns that can be readily instantiated. Currently, there are also novel approaches focusing on enable cross-functional collaborative threat modeling, such as the work proposed by Von der Assen et al. (2022) that applies existing threat modeling methodologies (*e.g.*, STRIDE and DREAD) in a collaborative setting, thus, resulting in an approach that allows organizations to extend threat modeling to non-technical stakeholders in an automated way.

Also, there are multidisciplinary efforts focusing on address cybersecurity planning challenges. For example, inspired by the Project Management field, the work proposed in by Teufel et al. (2020) modeled an easy-to-use cybersecurity canvas to address the problem of SMEs having a lack of knowledge to handle cybersecurity. The proposed framework is based

on modular building blocks that can be individually or together according to the demands of an SME. This work uses a top-down approach divided into five layers. This helps companies use the framework as an initial self-assessment to think about processes and complexities to determine or improve a cybersecurity strategy. However, although the steps are well-defined and the framework easy to use, it does not indicate which kind of information an organization has to collect nor which kind of techniques and tools are needed for a successful assessment. Also, the outputs of the framework are hard to measure since there is no indication of what is a success/failure for each layer.

Therefore, there are efforts on different fronts to achieve better cybersecurity in companies, but there is still a lack of approaches that guides SMEs during the different steps required for the planning and implementation of cybersecurity strategies. Thus, novel interdisciplinary approaches, methodologies, and guidelines are required to help SMEs define their requirements, manage the costs, and project risks while implementing cybersecurity strategies.

Cybersecurity economics also has a key role for cybersecurity planning and must be considered in the process, especially for the cost management. At the beginning of the 21st century, the main discussions and models for cybersecurity economics rose. Ross (2001) argued that the information insecurity is at least as much due to perverse incentives. One year later, in 2002, the GL model was proposed as an economic model that determines the optimal amount to invest in protecting a given set of information.

After a few years, the ROSI model was introduced in 2005 to be used as a benchmark methodology to support cybersecurity decisions by performing a cost-benefit analysis of protections. These two models are still the most accepted today. Ross and Moore (2006) also provided an insightful discussion regarding the advances and challenges of cybersecurity economics, highlighting that cybersecurity economics goes into more general areas, such as system designs, management aspects, and privacy concerns.

3 Material and methods

For the development of this study, besides the mapping of the critical processes and information, it is essential to consider the different stakeholders and personnel of the company, such as the directors, project managers, and employees that operate critical activities. These stakeholders might be, for example, a target for social engineering attacks and even insiders.

The methodology used to propose the SECProject framework considers a qualitative approach, as previously discussed by Franco & Lacerda (2021), focusing on the processes, tasks, and information required for the design of our framework. Initially, a literature review was conducted to identify the most common threats and challenges for SMEs. Next, an analysis of each of these threats' economic impacts has been conducted using the steps defined by the SEConomy framework, as proposed by Rodrigues et al. (2019). Finally, state-of-the-art approaches, as mapped in Section 2, and key steps to reduce the risks and costs of executing cybersecurity projects (acquisition, training, operation) have been investigated.

In a second step, the SECProject framework was designed considering the mapped elements and the different project management techniques discussed in the literature, mainly focusing on risk and cost management (Project Management Institute, 2017). For that, different models from cybersecurity economics, such as Return On Security Investment (ROSI) (Sonnenreich, Albanese & Stout, 2005) and the Gordon-Loeb (GL) (Gordon & Loeb, 2002) models have been integrated with best practices for project management in order to provide a framework that guides decision-makers to where and how to invest in cybersecurity, while minimizing all risks and costs involved in the execution of projects to implant a cybersecurity strategy in companies with constraints in terms of budget, time, and technical expertise of both project and business stakeholders. For minimizing costs in cybersecurity projects, cybersecurity economic metrics have a key role in the decision making and planning of all requirements that leads to an effective cybersecurity strategy.

The evaluation of the SECProject relies on the foundations of the case studies approach. Case studies can be described as a qualitative approach highly iterative and tightly linked to data, which is appropriate in new topic areas where qualitative evaluations are preferred (or the only possible) instead of quantitative ones (Harrison et al., 2017). Furthermore, it is worthy of highlighting that case studies have an important role in scientific development (Flyvbjerg, 2006). Whether well-defined, it can be generalized for others scenarios, thus providing examples of the feasibility and applications of approaches, systems, and methods. Also case studies help to validate the framework, while circumvent possible limitations regarding information sharing in cybersecurity.

All decisions took to propose the SECProject framework are fully considering the real-world demands as basis, including official reports and surveys. For the process of data collection, it was considered official information from Swiss government regarding SMEs as

well as interview with different stakeholders, including interviews with four CEOs of Swiss SMEs working directly with innovation, and nine risk analysts and cybersecurity insurance underwriters based in Europe and United States. Those interviews were composed by Likert-scale questions regarding the importance of cybersecurity for their companies as well as their current strategies and challenges. Also, open questions regarding specific demands for novel solutions and current solutions used in their companies were asked.

Results from the interviews shows lack of cybersecurity awareness, budget, and information protection in all of the interview companies. Also, all of them just have basic cybersecurity deployed (e.g., antivirus and firewall) and none of them have a clear defined recovery plan in case of cyberattack. This results are in full aligned with the survey conducted by ENISA (2021) with 250 SMEs in Europe, showing the different factors impacting SMEs cybersecurity and challenges. Also, by interviewing five cybersecurity underwriters in the context of this study, it was identified that most of the analysis conducted by cybersecurity insurers for definition of insurance premium relies on a self-assessment questionnaire filled by the customers, and only in most critical scenarios a security audit and penetration is conducted. The results of the interviews with cybersecurity underwriters are described in Matejka, Soto & Franco (2021). All of the interviews conducted and analysis highlights the importance of approaches that helps SMEs to improve and understand cybersecurity, since the entire ecosystem relies on that. This provides insightful information to guide the definition of the phases and steps that composes the proposed framework.

The evaluation of the framework is based on the practical application of the framework in a company as a case study. A case study was defined here as the evaluation method due to the limited information sharing in the cybersecurity field since this kind of information is (a) critical for companies in a way that they cannot sharing or (b) the companies do not have all information at hand due to lack of technical expertise. Also, qualitative evaluations like case studies can highlight the benefits of the framework and help companies to apply then for further quantitative evaluations. An additional case study for SECProject is also provided by Franco & Lacerda (2021).

For this case study, it was defined a company based on the reality of the Swiss market for SMEs. The numbers for that are provided by a national study conducted in 2019 by the Swiss Federal Office for Statistics (Swiss SME Portal, 2021). Considering the market facts, a

hypothetical company was defined for this case study. This company is considered hypothetical but supported by information and scenarios from the real Swiss SMEs.

This hypothetical company is the PARME Pharma AG, a small-sized pharmaceutical company with 27 employees based in Basel, Switzerland. The main business of this company comprises the development and testing of new pharmaceuticals, chemicals, and cosmetics. The company works in a Business-to-Business (B2B) business model, thus, selling input production directly to other companies to develop their products and medicines for drug stores. Table 1 summarizes the numbers and business of the PARME AG.

Table 1.

Example of information of the company being considered as input for the SECProject

Information	Value	Description
Sector	Pharmaceutical Industry	Important information to be considered, since it gives indication about possible cyberattacks that might target specific sectors
Employees	25-30 people	Describes partially the size of the company, thus, helping to decide for strategies that fits better
Revenue	US$ 15 million yearly	The revenue and financial metrics are important to understand the value of the business, its assets, potential budget for investments, and also its market value
Country	Switzerland	Helps to understand the scenario and which regulations have to be followed when implementing cybersecurity strategies
Portfolio	Development, test, and distribution of pharmaceuticals and cosmetics	Overview of the products and possible impacts of cyberattacks in the company. It is important to consider during the risk management tasks

Source: Original results from the research.

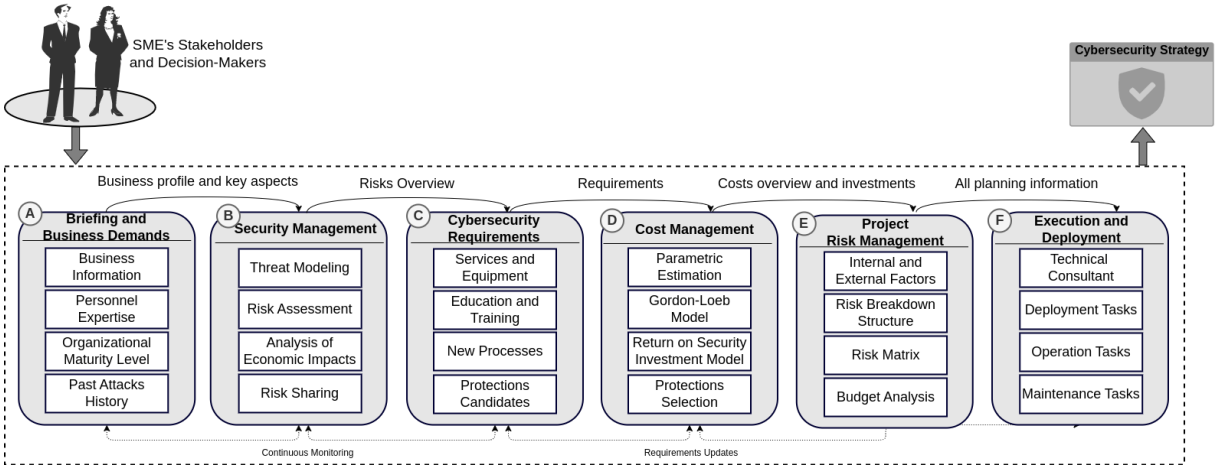
3 Results and discussion

Figure 1 provides an overview of the proposed SECProject framework, including the different phases and key steps to be considered. The framework starts in Phase A, where all information related to the business is collected and a briefing conducted with the stakeholders involved. Then, Phase B is focused on the security analysis and threat modeling of the company. For that, state-of-the-art tools, solutions, and approaches can be considered (Franco, 2023). Finally, with the information from the security analysis at hand, Phase C consists of the definition of the project requirements, the mapping of processes that have to be modified or created within the company, and also the definition of training required to implement, deploy, and operate the cybersecurity strategy.

After having all information mapped and the project requirements defined (e.g., what is the main goal, what is an acceptable level of protection, and which risks can be assumed), the Cost Management phase (Phase D) starts. In this phase, the project's costs are estimated, and the optimum investment amount is defined. For that, a parametric estimation can be conducted to determine the costs in terms of time and resources required to conduct the project. This step uses the company's historical data and successful projects implemented in companies with a similar environment. It helps to estimate, with a certain level of granularity, the resources and time required for the project execution.

Figure 1.

The SECProject Framework



Source: Original results from the research.

As SMEs does not have large experience with cybersecurity, it is possible to use both (a) information from others companies and partners with similar characteristics and (b) expertise in other IT projects that shows the costs to deploy, training, and operate new solutions. This, together with cybersecurity economic models, can be a very valuable resource to be used as an estimating tool with a reasonable level of accuracy. Example of aspects to be considered for the parametric estimation (*i.e.*, for the estimation of costs and time) of cybersecurity projects include:

- Historic and market data on the cost and time requirements to implement similar protections and training;
- Determine the maturity of the team to lead and implement the project;

- Determine the steps that are critical for the success of the project, which cannot be excluded from the budget available;
- The amount of solutions to be deployed and how large is the infrastructure to be protected (*e.g.*, number of end-points, computers, and network devices).

Still in the Cost Management phase, it is important to determine the maximum amount to invest in cybersecurity based on its value and data. For example, in some instances, it is more adequate to assume risks than invest a large amount of money in protecting not critical systems. In order to obtain this value, the SECProject framework applies the GL model, one of the most well-accept models for cybersecurity investments.

GL model determines that the investment in security should not exceed 37% of the potential loss *(Gordon and Loeb, 2002)*. The optimum investment is defined as the investment *z* that can maximize the Expected Benefit of Investment in Information Security (ENBIS). The ENBIS, as shown in Equation 1, considers the current vulnerability of system (v) minus the change on the vulnerability with additional investment (S(z, v)) and the potential loss (L). This calculation minus the invested amount determines the, which is exactly what have to be maximized to find the optimal investment in cybersecurity.

Equation 1.

Calculation Of The Expected Benefit Of Investment In Information Security

$$ENBIS(z) = \{[v - S(z, v)] * L\} - z \quad (1)$$

Source: Gordon, Loeb and Zhou (2021).

After obtaining the optimum amount of investment in cybersecurity, the next phase consists of determining which are the candidate solutions (firewalls, antivirus, and cloud-based services) and strategies (*e.g.*, employees training and backups) to be implemented, as mapped in the previous phases of the framework (*i.e.*, Project Requirements), using the budget available. For that, as proposed by Franco et al. (2019), recommender systems can be used together with other methodologies based on the technical know-how of the company.

After the solutions are mapped, the next phase consists of the analysis of the ROSI for each one of the solutions and strategies mapped to be implanted. This includes, for example, the calculation of ROSI for investment in solutions and additional tasks. The ROSI model is

introduced in Equation 2. The ROSI is considered satisfactory (*i.e.*, the investment is recommended compared to the potential loss) if it results in a number higher than 1.

The ROSI takes into account the Annual Loss Exposure (ALE), the mitigation rate, and the cost of the investment to assess if a solution is worth the investment or not. For that, the Single Loss Exposure (SLE) and the Annual Rate of Occurrence (ARO) have to be considered, which describes, respectively, the estimated cost of a security incident (*e.g.*, a data breach or a DDoS attack in the company) and the estimated annual rate of an incident occurrence (*i.e.*, based on the historical data and threat modeling, which are the probability of being attacked).

Equation 2.

Calculation Of The Return On Security Investment Metric

$$ROSI = \frac{((ALE \times MitigationRate) - Investment)}{Investment} \quad (2)$$

$$\text{where, } ALE = SLE \times ARO$$

Source: Sonnenreich et al. (2005).

The next phase in the SECProject framework consists of the continuous management of the risks of the project. It is important to have the information of the costs and investments possible, thus, helping to adjust the variables to achieve not only cost-effective cybersecurity but a feasible project to be implanted and operated by a company. For this phase, the first step focuses on the map of internal and external factors that can impact the project during its execution, such as lack of security expertise, stakeholders, regulation (*e.g.*, GDPR in Europe and LGPD in Brazil), and economic aspects (both direct and indirect losses).

After determining these factors, a tailored Risk Breakdown Structure (RBS) (Sato, Tanimoto & Kanai, 2020) for the project is provided. With the RBS, it is possible to represent the most relevant sources of risks for the cybersecurity project hierarchically, thus allowing for the identification and categorization of the risks to be considered during the planning and execution of the project. In the RBS, Level 0 represents all sources of project risks, while Level 1 provides the categories of risks. Level 2 shows the steps and tasks that involve risks.

Another important artifact to be generated to support risk management is the risk matrix. It is an analytical tool that can be used for risk evaluation, frequently used to evaluate the risks

of cyberattacks (Behnia, Rashid and Chaudhry, 2012). However, the SECProject focuses also on evaluating the risks of implementing a cybersecurity project and also integrating cyber threats modelling approaches. The different steps required to deploy and operate the cybersecurity strategy must be defined and analyzed in terms of its impact to the project execution (*e.g.,* Insignificant, Minor, Moderate, Major, and Critical). An insignificant impact, if not happens in a frequency that demands additional efforts, has low risk and is easily mitigated by well-defined processes, while a critical impact has mostly very high risks and might require abandoning the project.

Figure 2 provides an example of a risk matrix to be applied in the context of SECProject, highlighting the risks and their impacts according to their likelihood. For example, suppose the impact of a problem, if happen, is Major (*i.e.*, delays the schedule, considerable additional costs, and impact on the level of protection) and the chance of it happen is higher than 90%. In that case, the risk of that problem for the project is Very High (highlighted in red), which means that this might cause risks to the project that cannot be assumed and mitigation measures have to be taken.

Figure 2.

Example Of An Adapted Risk Matrix For The Secproject Framework

		Impact				
		Insignificant (Insignificant impact and can be mitigated)	**Minor** (Delays the schedule up to 10% and/or additional costs are possible)	**Moderate** (Delays the schedule up to 30%, reasonable additional costs, and/or might impact in the level of protection)	**Major** (Delays the schedule up to 50%, considerable additional costs, and/or impact in the level of protection)	**Critical** (Catastrophic, the project becomes not feasible and has to be abandoned due to economic and technical reasons)
Likelihood	Certain > 90% chance	**High**	**High**	**Very High**	**Very High**	**Very High**
	Likely 50%-90% chance	**Moderate**	**High**	**High**	**Very High**	**Very High**
	Moderate 10%-50% chance	**Low**	**Moderate**	**High**	**Very High**	**Very High**
	Unlikely 3%-10% chance	**Low**	**Low**	**Moderate**	**High**	**Very High**
	Rare < 3% chance	**Low**	**Low**	**Moderate**	**High**	**High**

Source: Original results of the research.

It is essential to mention that Cost and Risk Management are complementary phases, which can be adapted according to the company's requirements until a feasible project is defined. The SECProject framework then provides a clear path and rich information to be used as a basis during the project execution and cybersecurity deployment phase.

The last phase of the proposed framework is the Execution and Deployment. At this phase, the company already has different artifacts and information, provided by early phases, to manage the execution and deployment of the cybersecurity project with a clear view of its risks, costs, goals, and success rate. In the light of this information, the company can then define requirements for an external technical consultant or schedule the different technical tasks required for the effective deployment and configuration of the new cybersecurity strategy adopted by the company. Also, operation and maintained tasks have to be mapped at this last step in order to have not only adequate protection but also an efficient plan to manage and operate the entire system, which might require additional training, employees, and equipment that fits the budget previously defined in the cost of the project.

3.1 Case study: definition of a cybersecurity strategy using the secproject framework

This case study focuses on mapping the stakeholders, threats, and cost-efficient strategies to plan the safe operation of a new E-Commerce system of PARME AG. This system can result in more competitiveness in the market for PARME but introduces new challenges due to potential financial losses due to cyberattacks. For that, the SECProject framework will be applied, supported by different state-of-art solutions available on the literature to achieve a cost-efficient strategy that fits the requirements of the company.

All information required for this case study was obtained from four different sources: *(i)* public information from the Swiss market, *(ii)* reports available regarding cybersecurity trends and threats for specific sectors, *(iii)* interviews and discussions with cybersecurity experts and SMEs employees, and *(iv)* arbitrary information based on a literature review to fulfill gaps of information that are not possible to be obtained from the others sources.

Phase A. Briefing and Business Demands. The framework starts in Phase A, where all information related to the business has to be collected and a briefing conducted among the company decision-makers. For that, the information mapped previously in Table 1 is considered. This information is based on example of companies in Switzerland from the same sector and also the reality of the Swiss market (Swiss SME Portal, 2021). This gives initial insights into the sectors and size of the company. Next, the personnel expertise of the company is analyzed as an indicator to understand possible challenges or technical weaknesses to be considered during the planning of a cybersecurity strategy.

In the case of PARME AG, the employees allocated and contracted to work in the E-Commerce department have low awareness of cybersecurity. However, they have basic skills to operate computers, since they perform different daily activities, such as navigating the Internet, processing sales requests, and using office suites. Most employees have a bachelor's degree in a non-related technology field. Therefore, based on that information, it is possible to assume that the employees have a high level of education but without too much information technology background. This lack of background can be explored as an attack vector in the future; therefore, this has to be considered for the planning of cybersecurity strategies.

Understanding the maturity level of the business and its processes is also important during this initial phase, since it can highlight possible weaknesses/strengths to adapt to new processes introduced by a cybersecurity strategy. In the case of PARME AG, it is a company operating for over 15 years, with processes well-defined defined in the pharmaceutical sector. However, information technology is still being validated, since the company's E-Commerce platform is very recent. Therefore, there is still a path to follow to integrate and control all current and new processes, which is still a more significant challenge without contracting dedicated technical people to handle that.

Finally, the history of past attacks on the company has to be considered. This is an important metric, since it can have a key role in adopting the cybersecurity strategy combined with other statistics and security trends. However, this information is very sensible and confidential for companies to avoid malicious attackers from exploiting it. Therefore, based on a literature review and the most common attacks on the company's sector, the following information has been considered valid for the last three years:

- The PARME AG had a yearly average of five phishing attacks, and three Malware attacks;
- The success rate was respectively 15% (Phishing) and 10% (Malware), which means a percentage of these attacks impacted the company in an economical and technical way;
- Although this information shows possible attack vectors, no critical impacts on the operation of the business were identified in the past.

This information can trigger alerts for the rest of the planning steps. While the company did not face any critical impact in the past, there are high success rates for these attacks. Also, the number of attacks might increase, additional cyberattacks (*e.g.*, DDoS and Ransomware), and the company becomes more digitally exposed to E-Commerce businesses. For example, a

phishing attack can be used to infect the entire company infrastructure with a Ransomware attack and cause business disruption, leak of customers' data, and financial loss due to data recovery. Also, DDoS attacks can target E-Commerce directly to put the system down and impact the revenue and reputation of the company directly (Franco et al., 2020). Thus, it is important to have this past attack history in mind and map possible risks and threats during the next phase.

Phase B: Security Management. For the security risk analysis, three company's assets are to be taken into consideration: *(i)* the E-Commerce Web Server, which is responsible for maintaining the platform running, *(ii)* the E-Commerce platform, which provides all features for the user to interact and buy products from PARME AG, as well as allow the PARME AG employees to manage the logistics and the financial processes, and *(iii)* the databases that store information about customers, payments, and products.

Also, the stakeholders have to be mapped. Stakeholder is any individual or group that cyberattacks in the system can affect. Therefore, for this case study, the stakeholders are the *(i)* PARME AG decision-makers, *(ii)* customers, *(iii)* companies part of the PARME AG supply-chain, and *(iv)* infrastructure manager of PARME AG. The threat sources are defined as of in Hofmann (2019). Therefore, employees may cause intentional and unintentional damage, amateur and skilled hackers can exploit vulnerabilities for financial advantage or sabotage, and competitors might hire someone to damage the company's reputation.

The threat modeling is then conducted, taking this information into account. Also, the Open Web Application Security Project (OWASP) vulnerabilities and trends for the sector are considered during this step. Table 2 summarizes the main threats identified, including their likelihood of happening, possible economic impacts on the company, and also which dimension of the STRIDE framework (Xiong & Lagerstrom, 2019) the threat is classified.

Table 2.

Overview Of Threats That Might Face The Company And Their Possible Impacts

Threat	Likelihood	Economic Impacts	STRIDE Classification
T1: DDoS	Likely	LR, CM, and RH	Denial-of-Service
T2: Phishing Campaing	Likely	CR	Spoofing, Information Disclosure
T3: Ransomware	Moderate	LR, CR, RH	Denial-of-Service, Information Disclosure
T4: Insiders and Supply-Chain Attacks	Moderate	LR, CM, RH	Repudiation, Information Disclosure, Elevation of Privilege
T5: Cross-Site Request Forgery (CSRF)	Moderate	CM	Spoofing, Privilege Escalation
T6: SQL Injection	Not Likely	RH, LC	Tampering, Information Disclosure

Note: Loss in Revenue (LR), Costs for Mitigation (CM), Reputation Harm (RH), Legal Costs (LC).
Source: Original results of the research.

A total of six Threats (T) were identified, named from T1 to T6. The selection of these threats is based on the risk assessment previously conducted on the company and the trend of specific cyberattacks in the company's sector. Also, four major economic impacts were considered: Loss in Revenue (LR) due to business interruption, Costs for Mitigation (CM) before or during an attack, Reputation Harm (RH) due to a successful attack, and Legal Costs (LC) associated to third-party impacts and data breaches. Note that the LR and CM are examples of direct impacts of a cyberattack, while the RH and LC are indirect impacts.

Next, a risk analysis is conducted to highlight the threats that introduce more risks for the business in terms of economic, technical, and legal impacts. A risk assessment matrix is built, considering two different scales: Likelihood and Impacts. Based on that, it is possible to map the risks of each threat as Low, Medium, and High. For example, one threat that have a Moderate likelihood of happening but the impacts are Acceptable is classified as Low risk. On the other hand, a likelihood defined as Likely and impact as Tolerable is classified as High risk.

The risk assessment matrix for PARME AG can be then created, taking as input all of the six threats initially mapped. The most critical threats (*i.e.*, High risk) are the T1 (DDoS), T2 (Phishing), and T3 (Ransomware). The threats T4 (Insiders and Supply Chain Attacks) and T5 (CSRF) have also to be considered, since they have a Medium risk. The T6 (SQL Injection) does not offer too much risk (in terms of likelihood vs. impacts), therefore should not be the priority at this step. Based on threat modeling and risk analysis, it is determined what is critical and the priorities to achieve the level of protection needed. Thus, by analyzing this information, the conclusions to be taken into consideration are the following:

- The risk of phishing and ransomware is increasing, and it has become one of the most significant threats for the company. Training and Protections are a must;
- DDoS attacks are one of the biggest threats to the availability of the E-Commerce platform. Protections are a must;
- Insiders and Supply Chain attacks are also a cause of concern, and new processes and protections have to be defined to reduce their possible impacts;
- Training and education of employees have to be done focusing on the most common threats identified for the company;
- Best practices of development and tests have to be applied to avoid threats like CSRF, Cross-Site Scripting (XSS), and others Web Application security risks.

Phase C: Cybersecurity Requirements. After the briefing and analysis of all threats and risks, it is now required to determine the cybersecurity requirements of the company. This includes services and equipment required, additional training for the employees, and the definition of new processes that have to be implemented by the PARME AG to have a proper strategy to run their E-Commerce safely. The decision-makers define these requirements during the planning of the cybersecurity strategy. Table 3 summarizes all of the cybersecurity requirements. These requirements are looked into because of the company's characteristics and initial demands. However, different requirements can be considered according to the initial information collected during the briefing and brainstorming (*i.e.*, Phase A).

The requirements are defined from R1 to R7, including constraints defined by the business team, and possible providers for these kinds of solutions are mapped. With the requirements defined and possible providers available in the market, it is possible to estimate the costs and determine how to ensure the cybersecurity strategy's economic feasibility.

Table 3.

Overview Of Defined Requirements For PARME AG And Possible Service Providers

Requirement	Constraints	Possible Providers
R1: Cloud-based DDoS Protection	Must be cloud-based and provide defenses against at least SYN, ICMP, and UDP flood	Arbor, Verisign, Akamai, and Cloudflare
R2: Email security and phishing protection	No constraints	Proofpoint, Abnomrla Security, IronScales, and Barracuda
R3: Software against viruses and malware	Must provide endpoint security protection for all computers connected in the company's network	Symantec, McAfee, Microsoft Defender, and Bitdefender
R4: Implement a monitoring and logging strategy	Must be stored out of the company premises	-
R5: Security audit and code review before deployment of new features on the company's solutions	Must consider all of the stakeholders, threats, and risks mapped for the business	Internal analysis, consultancy companies, and security experts
R6: Monthly updates for critical software and semiannual updates for others software	All software must run the last stable version with the most recent security patches	-
R7: Education and training of employees against phishing and Social Engineering attacks	Must have online courses contracted for continuous education and face-to-face training for selected threats	Coursera, consultancy companies, and Swiss universities

Source: Original results of the research.

Phase D: Cost Management. It is important to determine how much budget must be available for this phase as an initial step. This amount can be achieved by applying the GL model. For this case study, the GL model is applied to calculate two different values: the *(i)* maximum budget for cybersecurity and *(ii)* optimum investment per segment (*i.e.*, assets). This helps the company have a broad understanding of how to determine their budget and the costs of the cybersecurity strategy.

The company's total revenue was previously determined as US$ 15 million yearly, and the E-Commerce itself as a value of US$ 5 million for the company. Therefore, this last will be considered as the potential loss if a successful attack happens in the E-Commerce and underlying infrastructure. Without any investment, based on the risk analysis previously conducted, the risk of an attack happening is equal to 64%, and the success rate is equal to 41%. This information is related to the worst scenario possible. Thus, the GL model equation for maximum investment successful attacks is applied. This means to calculate 37% of following: the asset value (US$ 5M) times the risk of being attacked (64%) times the success rate of attacks (41%). Thus, PARME's investment in cybersecurity should not exceed US$ 485,440 annually.

This calculation indicates the maximum budget but is still not the optimum investment possible. In order to calculate the optimum investment, the SECAdvisor tool proposed by Franco (2023) and available at https://secadvisor.figueredofranco.com is used. The SECAdvisor can help with this task by applying the different equations of the GL model in a user-friendly and automated way. Table 4 shows the optimal investment calculated for three different segments of PARME AG. This case study focuses on the first one: The E-Commerce running as a Web Server. For this one, with a value estimated at US$ 5,000,000 (total yearly revenue), the optimal investment calculated is equal to US$ 75,623. This means that the optimal amount to protect the E-Commerce platform is roughly only 15% of the maximum investment previously calculated. It is important to state that in the backend, the SECAdvisor tool is running the GL equations and security breach probability functions as defined by Gordon, Loeb & Zhou (2021).

With this amount now at hand, it is possible to start the search to satisfy all seven requirements by spending not more than US$ 75,623 annually. R1 (Protection against DDoS attacks), R2 (Email security), and R3 (Antivirus) need a decision about which of the protections available are more suitable in terms of technical and economic demands. After define possible protections candidates, the ROSI model can be applied to determine which is the most cost-efficient protection.

Table 4.

Optimal Investment For The PARME AG Segments Calculated Using GL Model With The Support Of The Secadvisor Tool

Segment	Type	Risk	Vulnerability	Value	Optimal Investment
E-Commerce	Web Server	64%	41%	$ 5,000,000	$ 75,623
Databases	Database	51%	43%	$ 2,000,000	$ 27,665
Internal Network	Network	6%	12%	$ 20,000,000	$ 43,246

Source: Original results of the research.

For example, the loss due to DDoS attacks is measured as US$ 2,000 per hour of the attack, with an average of seven days of the week. This means an incident costs US$ 144,000. Based on this information and protection characteristics, the calculation of ROSI can be performed. Suppose the Verisign DDoS Protection has a mitigation rate equal to 80% of DDoS attacks and the cost of the solution equal to US$ 3,700 per month. The ROSI calculation for

this solution is equal to 7 (rounded), which means that the payback on this investment is 700%. This is an excellent ROSI and means this is a cost-effective solution. This calculation can be done to all protections to determine which one fits better the budget. Table 5 summarize all costs mapped to achieve the requirements of the company in terms of the level of security, considering the best approaches selected in terms of performance and costs.

Thus, after the costs calculations, the amount to plan to invest in a cybersecurity strategy that fits all requirements of the company is equal to US$ 58,300. This amount is 78% of the optimal investment previously defined by the GL model. Therefore, there is still an amount of ~US$ 17,300 that can be used to address additional requirements or to be invested to cover not expected costs during the deployment and operation of the cybersecurity strategy, such as contract consultancy and experts to support and train the company's team in specific activities. Also, this amount can be used to buy additional equipment if needed or to increase the IT team (e.g., allocate people partial time to work on security aspects of the company).

Table 5.

Summary Of Costs To Address All Requirements Of The Cybersecurity Strategy

Investment	Requirement Covered	Provider	Product	Cost (Yearly)
Protection against DDoS	R1	Verisign	DDoS Mitigation Service	US$ 44,400
Email security	R2	Barracuda	Premium Email Protection	US$ 1,800
Anti-Virus and Anti-Malware	R2 and R3	Bitdefender	GravityZone Business Security	US$ 3,000
Storage and management of critical logs	R4	SolarWinds	LogEvent Manager	US$ 1,900
Security analysis and code verification	R5	PwC Switzerland	Source Code Analysis	US$ 10,000
New process for continuous update and upgrade of software	R6	SolarWindws	Patch Manager	US$ 2,000
Online security awareness education and on-site training	R7	Course and University of Zurich UZH	Cybersecurity Awareness Training and Hands-on	US$ 5,200
-	-	-	**Total**	**US$ 58,300**

Source: Original results of the research.

Phase E: Project Risk Management. In order to reduce that impacts in the execution, deployment, and operation of the project, it is required to analyze the risks and make

adjustments, if needed, in the previous costs (Phase D) and other planned steps before going to the last phase defined as Execution and Deployment.

Table 6 summarizes the risks identified to the cybersecurity project affected by time, costs, and performance. As highlighted in red, some risks can have a very high impact on the project, which might require additional actions. The technical risks can be mitigated by a check in the project requirements by a security expert as well as the map of the different complexities that the new processes might add to the employees. These complexities can be covered during the education and training of the employees, which is already covered by the requirements of the project.

As the budget defined in Phase D was not fully used, there is room for new investments, if required. This does not mean that the cybersecurity strategy was planned incorrectly, but can be used to cover externalities and uncertainties involved both cybersecurity planning (Fielder et al., 2018) and project management (Lima et al., 2022).

Finally, the regulations like GDPR and Cybersecurity Act do not have too much impact on the project since the company is already aware of and implementing most of these regulations, which there are no critical changes after the deployment of the cybersecurity strategy.

Table 6.

Summary of risks that might impact in the project being implemented

Type	Risk	Impact	Likelihood	Overall Risk
Technical	Insufficient level of protection	Critical	Unlikely	Very High
Technical	Technical process too complex for the employees	Major	Moderate	Very High
Management	Insufficient budget to achieve the minimum requirements	Critical	Unlikely	Very High
Management	Lack of in-house expertise to manage the execution and deployment of the project	Major	Moderate	Very High
External	Issues related to the adoption of the GDPR and Cybersecurity Act	Moderate	Rare	Moderate
Commercial	Partners and suppliers not able to adopt additional security steps for the supply chain	Minor	Unlikely	Low

Note: Overall risks in red means critical risks and green acceptable risks.
Source: Original results of the research.

Phase F: Execution and Deployment. Finally, the last phase of the framework involves executing and deploying the cybersecurity strategy. If not placed in the company already, technical support can be achieved by contracting consultants. Also, a clear deployment schedule

must be defined, since some company sectors might need to stop their operations for a few hours to deploy the solutions and new processes fully. After deploying the cybersecurity strategy, continuous operation and maintenance tasks have to be performed, such as continuous monitoring of critical activities and analysis of new threats.

After following in detail all of the phases and steps provided by the SECProject, the PARME AG was able to *(i)* define its cybersecurity demands based on the current company structure, *(ii)* determine the threats and risks of potential impacts (*e.g.,* economic losses and technical disruption) due to cyberattacks, *(iii)* describe the requirements to achieve an adequate level of protection according to its needs, and *(iv)* manage the costs to obtain a cost-efficient cybersecurity strategy. After deploying the strategy, the company is expected to achieve the right level of protection according to the demands to run its new E-Commerce business without putting critical risks to its assets, reputation, and revenue.

5 Conclusions and final remarks

This article proposed a six steps framework for the planning, definition, and execution of a cybersecurity project for SMEs. After the execution of such a cybersecurity project, the companies can achieve a better cybersecurity strategy to handle threats that affects both small, medium, and multinational companies around the world economically. For that, the SECProject framework explores concepts of the project management field to organized in a structured way the different concepts and demands of cybersecurity projects.

In conclusion, there is still room for novel frameworks and tools to support an efficient cybersecurity culture inside companies, including cybersecurity projects that lead to an adequate cybersecurity strategy. However, these approaches still have many challenges due to the lack of information regarding threats and relevant metrics for the planning and executing a cybersecurity project (*e.g.,* the time required to implement different strategies and the actual costs for companies to protect their businesses). Therefore, many assumptions still are required when applying frameworks as such proposed by SECProject. Still, it provides a clear path and good estimation to guide the adoption of better cybersecurity strategies by applying the state-of-the-art concepts from project management and cybersecurity economics.

The conducted case study highlights all of these elements and provides a practical application of the SECProject for a cybersecurity project execution in a company. During the case study, it is possible to observe that some assumptions are required according to the

information available. At the same time, the steps also can be reduced or extended to achieve the overall goal of implementing a cybersecurity strategy. This allows the extensibility needed to adequate the framework for scenarios with specific demands, where it is not possible to generalize all phases.

As future study, it is suggested (a) the design and development of a visual tool to support the calculations of the costs of the project based on cybersecurity economic models, (b) explore other project management concepts (e.g., agile and adaptive environments, DICE score, and mitigation measures) for a more tailored estimation of parameters related to the risks project's failures, and (c) extend the framework to support also the risk-sharing by contracting cyber insurance coverages provided by third-parties.

References

Behnia, A.; Rashid, R.; Chaudhry, J. (2012). A Survey of Information Security Risk Analysis Methods. Smart Computing Review, Vol. 2, No. 1: 79-94.

Cairns-Lee, H.; Lawley, J.; Tosey, P. (2022). Enhancing Researcher Reflexivity About the Influence of Leading Questions in Interviews. The Journal of Applied Behavioral Science, 58(1): 164–188.

CONCORDIA Consortium. (2022). Deliverable D4.3: 3rd Year Report on Cybersecurity Threats. Available at https://www.concordia-h2020.eu/wp-content/uploads/2022/07/CONCORDIA-D4.3.pdf. Accessed on: October 14 2022.

Cybersecurity Ventures. (2020). Cybercrime to Cost The World $10.5 Trillion Annually By 2025. Available at https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021. Accessed on: 18 April 2022.

Cynet. (2021). Survey of CISOs with Small Cyber Security Teams. Available at https://hubs.ly/H0FrnJ40.Accessed on: 18 April 2022.

European Digital Alliance. (2020). Skills for SMEs: Cybersecurity, Internet of things and Big Data for Small and Medium-sized Enterprise. European Commission, Brussels, Belgium.

European Watch on Cybersecurity & Privacy. (2021). Cybersecurity Label. Available at https://label.cyberwatching.eu/. Accessed on: October 24, 2022.

ENISA - European Union Agency for Cybersecurity. (2021). Cybersecurity for SMEs: Challenges and Recommendations. Available at https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes. Accessed on: October 12 2022.

Fielder, A.; König, S.; Panaousis, E; Schauer, S; Rass, S. (2018). Risk Assessment Uncertainties in Cybersecurity Investments. MDPI Games, Vol. 9, No. 2: 1-14.

Franco, M.; Rodrigues, B.; Stiller, B. (2019). MENTOR: The Design and Evaluation of a Protection Services Recommender System. In:15th International Conference on Network and Service Management (CNSM 2019), Halifax, Canada, October 2019, p. 1-8.

Franco, M.; Sula, E.; Rodrigues, B.; Scheid, E.; Stiller, B. (2020). ProtectDDoS: A Platform for Trustworthy Offering and Recommendation of Protections. In: International Conference on Economics of Grids, Clouds, Software and Services (GECON 2020), Izola, Slovenia, September 2020, p. 1–12.

Franco, M.; Lacerda, F. M. (2021). SECProject: A Framework for the Assessment and Management of Cybersecurity Projects in Small and Medium-Sized Enterprises. MBA Report, University of São Paulo, ESALQ/PECEGE, Piracicaba, São Paulo, Brazil. Available at https://figueredofranco.com/static/files/MBA-M-Franco.pdf. Accessed on: November 10 2022.

Franco, M. F.; Sula, E.; Scheid, E.; Granville, L. Z.; Stiller, B. (2022). SecRiskAI: a Machine Learning-based Approach for Cybersecurity Risk Prediction in Businesses, In: 24th IEEE International Conference on Business Informatics, Amsterdam, Netherlands, June 2022, p. 1-10.

Franco, M. (2023). CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment, PhD Thesis, University of Zurich, Zurich, Switzerland, February 2023.

Freiburg School of Management. (2019). Swiss International Entrepreneurship Survey: Results of the Study on the Internationalization of Swiss SMEs. Available at https://www.heg-fr.ch/media/mgkmsc4s/sies-report-2019_en.pdf. Accessed on: October 10 2022.

Flyvbjerg, B. (2006). Five Misunderstandings About Case-Study Research. Qualitative Inquiry, Vol. 12, No. 2: p. 1-27.

Gordon, L.; Loeb, M. (2002). The Economics of Information Security Investment. ACM Transactions on Information and System Security: 438-457.

Gordon, L.; Loeb, M.; Zhou, L. (2021). Investing in Cybersecurity: Insights from the Gordon-Loeb Model. Journal of Information Security: 49-59.

Harrison, H.; Birks, M.; Franklin, B.; Mills, J. (2017). Case Study Research: Foundations and Methodological Orientations. Qualitative Social Research, Vol. 18, No. 1: 1-17.

Hofmann, A. (2019). Security Analysis of the Blockchain Agnostic Framework Prototype. Independent Study, University of Zurich, Communication Systems Group, Department of Informatics, Zurich, Switzerland.

IBM Security, Ponemon Institute. (2020). Cyber Resilient Organization Report. Available at https://www.ibm.com/security/digital-assets/soar/cyber-resilient-organization-report/. Accessed on: August 2, 2022.

Kaspersky. (2020). Investment Adjustment: Aligning IT Budgets with Changing Security Priorities. Available at https://media.kaspersky.com/en/business-security/Kaspersky_IT%20Security%20Economics%202020_Executive%20Summary.pdf. Accessed on: June 14 2021.

Lee, I. (2021). Cybersecurity: Risk Management Framework and Investment Cost Analysis. Business Horizons: 1-34.

Lima, M. C. R.; Goussi, S. G.; Costa Borba, M.; Marinho, M. L. M. (2022). Management of Uncertainty in Projects and Its Strategies, Revista Visão: Gestão Organizacional: 48-61.

Liu, L.; De Vel, O.; Han, Q.; Zhangm, J.; Xiang, Y. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. IEEE Communications Surveys & Tutorials: 1390-1417.

Matejka, V.; Soto, J.; Franco, M. (2021). A Framework for the Definition and Analysis of Cyber Insurance Requirements. Master Project, University of Zurich, Communication Systems Group, Department of Informatics, Zurich, Switzerland.

National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity. Available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Accessed on: October 24 2022.

Qu, S. Q.; Dumay, J. (2011). The Qualitative Research Interview. Qualitative Research in Accounting & Management, 8(3): 238-264.

Presley, S.; Landry, J. (2016). A Process Framework for Managing Cybersecurity Risks in Projects. In: 19th Southern Association for Information Systems (SAIS 2016), Florida, USA, p. 1-4.

Project Management Institute. (2017). A Guide to the Project Management Body of Knowledge (PMBOK guide). 6th edition, Project Management Institute, Pennsylvania, USA.

Rodrigues, B.; Franco, M.; Parangi, G.; Stiller, B. (2019). SEConomy: A Framework for the Economic Assessment of Cybersecurity. In: 16th Conference on the Economics of Grids, Clouds, Systems, and Services (GECON 2019). Springer LNCS, Leeds, UK, p. 1-13.

Ross, A. (2001). Why Information Security is Hard - An Economic Perspective. In: 17th Annual Computer Security Applications Conference, New Orleans, USA, p. 358-365.

Ross, A.; Moore, T. (2006). The Economics of Information Security. Journal of Science, Vol. 314, Issue 5799: 610-613.

Sato, H.; Tanimoto, S.; Kanai, A. (2020). Risk Breakdown Structure and Security Space for Security Management. In: IEEE International Conference on Service Oriented Systems Engineering (SOSE), Oxford, UK, p. 7-16.

Sonnenreich, W.; Albanese, J.; Stout, B. (2005). Return On Security Investment (ROSI): A Practical Quantitative Model. Journal of Research and Practice in Information Technology: 239-252.

Swiss SME Portal. (2021). Figures on SMEs: Companies and Jobs. Available at https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/facts-and-figures/figures-smes/companies-and-jobs.html. Accessed on: October 12 2022.

Teufel, S.; Teufel, B.; Aldabbas, M.; Nguyen, M. (2020). Cyber Security Canvas for SMEs. In: 19th Internacional Information Security Conference (ISSA 2020), Springer, Pretoria, South Africa, p. 20-33.

Von der Assen, J.; Franco, M. F.; Killer, C.; Scheid, E. J.; Stiller, B. (2022). CoReTM: An Approach Enabling Cross-Functional Collaborative Threat Modeling. In: IEEE International Conference on Cyber Security and Resilience, Rhodes, Greece, July 2022, p. 1-8.

Xiong, W.; and Lagerstrom, R. (2019). Threat Modeling - A Systematic Literature Review. Journal of Computers & Security, Vol. 84: 53-69.