SECProject: a framework for the assessment and management of cybersecurity projects in small and medium-sized enterprises

Muriel Figueredo Franco[1]*; Fabricio Martins Lacerda[2]

[1] Communication Systems Group CSG. Department of Informatics IfI, University of Zurich UZH, Research Assistant, Binzmühlestrasse 14, CH-8050, Zurich, Switzerland
[2] PECEGE, ESALQ/USP. Profissional Associado, Doutor em Administração. Av. Pádua Dias, 11 – São Dimas; 13418-900 Piracicaba, SP, Brasil
* corresponding author: franco@ifi.uzh.ch

SECProject: a framework for the assessment and management of cybersecurity projects in small and medium-sized enterprises

Abstract

Cybersecurity remains one of the key investments for companies that want to protect their business in a digital era. However, most Small and Medium-sized Enterprises [SMEs] still misunderstand the threats and risks they are exposed to. Such a misunderstanding, associated with a lack of budget and technical expertise to implement an adequate cybersecurity strategy, results in more risks and, consequently, economic impacts and business disruption due to cyberattacks. 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 by the company. For that, this work proposes SECProject, a practical framework that, supported by key project management concepts, defines the most appropriate steps to be considered when planning and implementing a cybersecurity strategy in a company. The SECProject framework allows for even companies without technical expertise to optimize their cybersecurity investments while reducing their business risks due to cyberattacks. In order to show the feasibility and how to apply the proposed framework, a case study was conducted within a Swiss SME from the pharma and supply chain monitoring sector. Based on that, it is possible to highlight which information and artifacts are required for each Phase From planning a cybersecurity project until the deployment and operation of a cybersecurity strategy.

Keywords: cybersecurity; risk management; cost management; project management.

SECProject: um framework para análise e gerenciamento de projetos de cibersegurança em pequenas e médias empresas

Resumo

A cibersegurança continua a ser um dos investimentos chave para as empresas que querem proteger os seus negócios numa era digital. No entanto, a maioria das Pequenas e Médias Empresas [PME] ainda não compreendem bem as ameaças e riscos a que estão expostas. Tal mal-entendido, associado à falta de orçamento e de conhecimentos técnicos para implementar uma estratégia adequada de cibersegurança, resulta em maiores riscos e, consequentemente, impactos econômicos e interrompimento de seus negócios devido a ciberataques. Portanto, é essencial compreender os diferentes passos necessários para implementar uma estratégia adequada de cibersegurança, que pode ser vista como um projecto de cibersegurança a ser desenvolvido, implementado, e operado pela empresa. Para tal, este trabalho propõe o framework SECProject, que, apoiado por conceitos-chave de gestão de projetos, define os passos necessários para o planejamento e implementação de uma estratégia de cibersegurança em uma empresa. O framework SECProject permite que mesmo empresas sem conhecimentos técnicos especializados otimizem os seus investimentos em cibersegurança, ao mesmo tempo que reduzem os seus riscos comerciais devido a ciberataques. A fim de mostrar a viabilidade e como aplicar o framework proposto, foi realizado um estudo de caso numa PME suíça do sector farmacêutico e de monitoramento cadeia de suprimentos. Com base nisso, é possível destacar que informações e artefatos são necessários para cada passo desde o planejamento de um projecto de cibersegurança até à implantação e operação de uma estratégia de cibersegurança.

Palavras-chave: cibersegurança; gerenciamento de riscos; gerenciamento de custos; gerenciamento de projetos.

Introduction

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 (Rodrigues et al., 2019).

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 et al., 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., 2020).

However, even with the rising of cyberattacks, there is still a wrong perception of risks and a lack of cybersecurity investments from different companies. Today, Small and Medium-sized Enterprises [SME] are among the most affected sectors. 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., 2020), which involve identifying threats, planning the investments, and managing all tasks required to conduct projects that result in an efficient cybersecurity strategy (NIST, 2018).

Thus, the steps required to analyze the requirements and costs to implement cybersecurity strategies in SMEs are critical to achieving a proper level of protection for businesses and their customers (Franco et al., 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 frameworks and models (Presley and Landry, 2016) that help decision-makers consider essential elements to make the best decisions regarding cybersecurity strategies in their companies (Lee, 2021), thus resulting in a cost-effective and feasible project to be implemented for the protection of their businesses and customers. Therefore, 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 their businesses.

This work 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. The proposed framework consists of the following 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) Risk Management to identify and mitigate risks that leads the project to fail, and finally the (f) Execution and Deployment of the project. All of these pillars are described in details in this work. Also, a practical case study is conducted in a Swiss SME with leading role for the innovation and solutions for the supply chain monitoring in the pharma industry (Modum AG, 2017). As an outcome, this practical framework supports decision-makers plan and deploy efficient cybersecurity strategies in their companies, helping to understand the costs and risks that might result in a project's failure. The case study has been conducted to give evidence of the feasibility of the proposed framework. Additionally, a discussion on challenges and best practices for executing cybersecurity projects in SMEs are provided.

Material and Methods

There are two main questions to be answered during the work: (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? To answer these questions, 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 of the business (which might, for example, be a target for social engineering attacks).

Thus, the development of this work focuses 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 and key steps to reduce the risks and costs of executing cybersecurity projects (acquisition, training, operation) have been investigated. Also, discussions and information regarding the economics perspective of cybersecurity, provided by the European CONCORDIA H2020 project (Franco et al., 2019), are used to support the decisions and guide the development of this work since the CONCORDIA project focuses on built an strong European ecosystem of cybersecurity, thus providing insightful discussions and content on the technical, legal, and economics facets of cybersecurity.

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 et al., 2005) and the Gordon-Loeb (Gordon and 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 the risk management of the project's success, it was applied the Risk Breakdown Structure [RBS] tool (Sato et al., 2020). This approach helps to determine the project risks and possible barriers to the effective deployment of a cybersecurity strategy. For that, it was mapped different internal (*e.g.,* strategic, operational, and resources) and external (*e.g.,* economic and environmental) risks as well as ways to mitigate them when possible (Wanner, 2015). Also, the Cause and Effect Diagram (a.k.a. Ishikawa diagram) (Ishikawa, 1976) can be applied to illustrate the main reasons for fails of cybersecurity projects. Finally, a risk matrix was applied to determine key risks that can negatively impact cybersecurity projects' success.

For cost management, the PMBOK (Project Management Institute, 2017) has been used as the basis to determine the main steps required. For the first step, a cost management plan for cybersecurity was described using a parametric estimation. It describes the total cost

estimate of cybersecurity projects, considering the most important requirements and tasks. Information collected from 5,266 SMEs across 31 countries regarding their cybersecurity investments (Kaspersky, 2020) is used as a basis for this estimation. Also, the Gordon-Loeb and ROSI metrics were applied to determine the optimum investment in both Capital Expenditure [CAPEX] and Operation Expenditure [OPEX]. This provides better planning and helps to allocate an adequate budget for the project's success (in terms of money and protection). Besides that, a protection recommender system called MENTOR (Franco et al., 2019) is used to help during the final decision process about one specific protection or action. Thus, it is provided as an outcome, a cost-efficient cybersecurity strategy, followed by efficient management of relevant costs involved in the project. This methodology was defined to be the basis for a framework that supports the assessment and management of cybersecurity projects. Thus, the SECProject framework is introduced in the next section, with all its inputs, processes, and outputs described in detail.

The evaluation of the SECProject relies on the foundations of the case studies approach (Eisenhardt, 1989). 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.

Therefore, evaluation of the framework is based on the practical application of the framework in a real-world company as a case study. For that, it was selected a company in Switzerland that offers innovative solutions based on blockchain (Scheid et al., 2021) for supply intelligence and automation, such as the tracking and monitoring of cold chain for the pharma industry, where sensors can be placed in order to monitor the production and distribution of products that have to be maintained in a low temperature and with controlled characteristics along the whole supply chain (*e.g.,* medical drug distribution and vaccine supplies).

The analyzed company was founded in 2016, raising more than U$ 13 million after release an Initial Coin Offer [ICO] in 2017 (Modum AG, 2017). Currently, the company has around 20 employees and yearly revenue of US$ 1.5 million, obtained mainly by the offering of monitoring devices and a full-fledged platform for the management of the monitoring processes. Table 1 gives an overview of all of this information. It is important to note that this information was obtained based on publicly available data on the company's official website and technical reports (Stiller et al., 2020).

This company also has investments and actions in research and innovation to develop novel products for its portfolio. For example, in one of its projects, a blockchain-based system for cold chain monitoring named BC4CC (Stiller et al., 2020) was researched and prototyped, providing good results with the potential to be explored in the market as a product. This project was conducted from 2018 to 2020, funded by the Swiss Innovation Agency [Innosuisse], and developed in a partnership with the Communication Systems Group of the University of Zurich. Based on that, the next step requires, besides the technical expertise and market/product analysis, the planning and deployment of an efficient cybersecurity strategy to allow for a safe operation of this new system. Otherwise, the innovation can result in threats and failures that negatively impact the company in different dimensions (*e.g.,* economic losses, reputation harm, and business disruption).

Table 1 gives an overview of the business profile information to be considered as an input for the framework (most precisely for the Briefing and Business Demands phase). All this information is relevant for the different steps involved since the misunderstanding of the business (*e.g.,* sectors, portfolio, and revenue) and all technical aspects (*e.g.*, technologies, current projects, and security risk analysis) can lead to a wrong project definition and management, thus resulting in an ineffective cybersecurity project (*e.g.,* wrong investment in cybersecurity, fails to deploy the project, an insufficient level of protection for the business).

Table 1. Overview of Information of the Company being considered for the Case Study

Metric	Value	Description
Sector	Supply chain monitoring, Pharma industry	The company sector is an important metric to be considered since it gives clues about cyberattacks that targets more specific sectors.
Technology	Blockchain and Internet-of-Things [IoT]	The technologies being used for the company can guide during the risk analysis for security threats and also to understand the value/amount of information handled by the company.
Employees	25-30 people	The number of employees describes partially the size of the company, thus helping to decide for strategies that fits SMEs or MNEs, for example.
Revenue Initial Coin Offer [ICO]	~US$ 1.5 million in 2020 ~US$ 13 million in 2017	The revenue and others financial metrics (*e.g.*, the ICO and tokens available) are important to understand the value of the business, its assets, potential budget for investments, and also the market value.
Country	Switzerland	The country where the company is placed helps to understand which regulations have to be followed when implementing cybersecurity strategies (*e.g.*, GDPR and Cybersecurity Act for Europe).
Portfolio	Monitoring Sensors and Full-Fledged Platform for Supply Tracking	This information gives an overview of the products and possible impacts of cyberattacks in the company. It is important for the risk analysis and threat modeling tasks.

Source: Original data of the research

Note that besides this information that defines the business profile, technical information is also considered and mapped, such as the current protections already placed in the business, the known threats, and the past attacks observed in the company. All required information is explored in-depth in the Results section.

The case study then focuses on mapping the company's stakeholders, threats, and cost-efficient strategies to plan the safe operation of the new blockchain-based system proposed by the BC4CC, which can result in more competitiveness in the market. This includes, for example, the definition of project requirements, the calculation of the optimal budget to invest in cybersecurity, and the selection of protections to be acquired/contracted. For that, the SECProject framework (*cf.* Figure 1), as introduced in the next section, is applied.

All of the information required for the case study was obtained from four different sources: (i) public information from the official company website, (ii) interviews with the team involved in the system development and companies decision-makers (*e.g.,* Chief Executive Officer [CEO] and Chief Financial Officer [CFO]), (iii) official documents published by the company and its developers as technical reports and scientific papers, and finally (iv) arbitrary information based on a literature review to fulfill gaps of information that are not possible to be obtained from the others mentioned sources.

Results and Discussion

This section presents the different contributions of this work and a practical case study to show the feasibility of the work in real-world scenarios. First, the proposed framework is introduced, with all of its phases explained and discussed. Next, a case study is presented to show the framework's application in a scenario of a Swiss SME, with all details of the performed steps and required information described. Thus, in this section, all of the artifacts, contributions, and challenges of the SECProject are discussed with different levels of abstractions.

The SECProject Framework

Figure 1 provides an overview of the proposed 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, such as the SEConomy framework and specific penetration tests. Finally, with the security information 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 is 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 that.

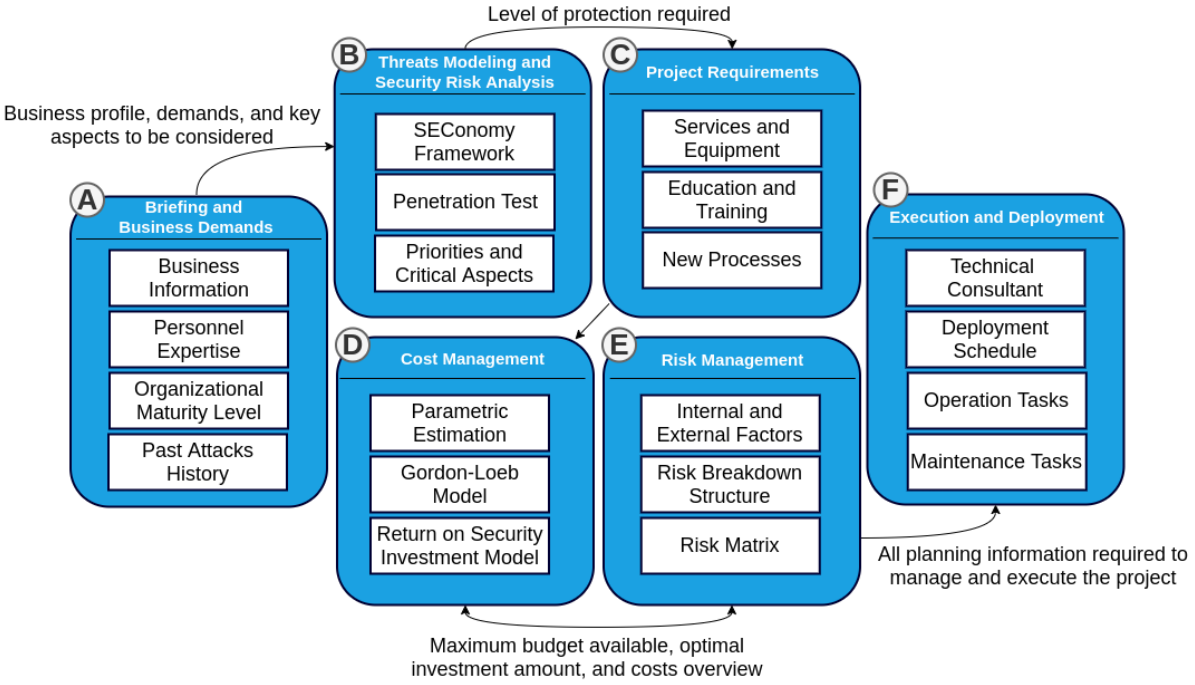


Figure 1. The SECProject framework
Source: Original results of the research

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 sectors and (b) expertise in other IT projects that shows the costs to deploy, training, and operate new solutions. This, together with other models presented below, can be very useful 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).

Taking this information and metrics into account, it is possible to apply the parametric estimating formula for each of the relevant metrics to have a view about the cost estimation of the project, which can be then correlated with the optimum investment and ROSI, as explained below. The parametric estimating formula is defined in eq. 1.

$$E_{Parametric} = \frac{A_{old}}{P_{old} \times P_{curr}} \quad (1)$$

where, A_{old}: historic amount of cost or time; P_{old}: Historic value of the parameter; P_{curr}: Value of that parameter in the current project

Source: Project Management Institute (2017)

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 Gordon-Loeb model, one of the most well-accept models for cybersecurity investments.

Gordon-Loeb determines that the investment in security should not exceed 37% of the potential loss (*d*). It relates to how much the system is valued (λ), how much the data/system is at risk (*t*), and the probability that an attack on the data/system is going to be successful (*v*). eq. 2 describes how to use this information for the calculation.

$$Investment = d \times 0.37 \quad (2)$$

where, $d = \lambda \times t \times v$

Source: Gordon and Loeb (2002)

After obtaining the optimum amount of investment in cybersecurity (*i.e.*, the Gordon-Loeb calculation), 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 implanted, as mapped in the previous phases of the framework (*i.e.*, Project Requirements), based on 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 (*e.g.*, firewalls, antivirus, and cloud-based services) and other tasks (*e.g.*, training and backups). The ROSI model is introduced in eq. 3. 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 the estimated cost of a security incident respectively (*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). All of this information has to be investigated in Phases A, B, and C. Furthermore, the cost of the investment and the possible proactive mitigation (*i.e.*, how much of the attacks can be avoided or mitigated by implementing the solution.

$$ROSI = \frac{((ALE \times MitigationRate) - CostoftheInvestment)}{CostoftheInvestment} \quad (3)$$

where, ALE=SLE×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 adjusts the variables to achieve not only cost-effective cybersecurity but a feasible project to be implanted and operated by the company. For this phase, the first Phase Focuses on the map of internal and external factors that can impact the project during its execution, such as lack of security expertise, stakeholders, legislation (*e.g.*, GDPR in Europe and LGPD in Brazil), and economic aspects.

After determining these factors, a tailored Risk Breakdown Structure [RBS] 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. Figure 2 shows an example of RBS for a generic project. For this example, Level 0 represents

all sources of project risks, while Level 1 provides the categories of risks. Then, Level 2 shows the tasks that involve risks.

RBS LEVEL 0	RBS LEVEL 1	RBS LEVEL 2
0. ALL SOURCES OF PROJECT RISK	1. TECHNICAL RISK	1.1 Scope definition
		1.2 Requirements definition
		1.3 Estimates, assumptions, and constraints
		1.4 Technical processes
		1.5 Technology
		1.6 Technical interfaces
		Etc.
	2. MANAGEMENT RISK	2.1 Project management
		2.2 Program/portfolio management
		2.3 Operations management
		2.4 Organization
		2.5 Resourcing
		2.6 Communication
		Etc.
	3. COMMERCIAL RISK	3.1 Contractual terms and conditions
		3.2 Internal procurement
		3.3 Suppliers and vendors
		3.4 Subcontracts
		3.5 Client/customer stability
		3.6 Partnerships and joint ventures
		Etc.
	4. EXTERNAL RISK	4.1 Legislation
		4.2 Exchange rates
		4.3 Site/facilities
		4.4 Environmental/weather
		4.5 Competition
		4.6 Regulatory
		Etc.

Figure 2. Example of a generic Risk Breakdown Structure
Source: Project Management Institute (2017)

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 on evaluating the risks of implementing a cybersecurity project, not the cyber threats. 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 3 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 issue, 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% (*i.e.*, Certain). In that case, the risk of that issue 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.

		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**

Figure 3. Example of an Adapted Risk Matrix for the SECProject Framework
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 (Schmit and Roth, 1990). 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 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 good protection but also an efficient plan to manage and operate the whole system, which might require additional training, employees, and equipment that fits the budget previously defined in the cost of the project.

Case Study: Application of the SECProject for the Protection of an SME

For this case study, as introduced in the Section “Material and Methods”, it is being considered a company that provides innovative solutions for the supply-chain tracing, with main focus on the Pharma industry (*e.g.*, components for medicines, vaccines, and hospital equipment). The case study consists of apply all of the steps defined by the SECProject

framework (*cf.* Figure 1) in order to build a cost-efficient cybersecurity strategy to be deployed in the company under investigation. It is important that many assumptions have to be done for the completeness of the case study. However, ever than possible, real-world information is used based on publicly available information, interviews, and published literature. These steps, all of the relevant information, and generated artifacts are described in the rest of this section.

Phase A: Briefing and Business Demands

The first step includes defining all relevant business information to understand what the business is and how it operates. For that, the information already mapped in Table 1 is the key. Next, the personnel expertise is an important indicator to understand possible challenges or technical weaknesses to be considered during the planning of a cybersecurity project. For the case of this company, the employees are very technology-oriented, with most of them with basic skills in computer networks and blockchain. Most employees have at least a bachelor's degree in a technology-related field (*e.g.*, Computer Science, Business and Informatics, Computer Engineering, and others).

Therefore, based on the high level of education and technical knowledge involved, it is possible to conclude that the company's capacity to adopt new processes and strategies that require technology is very high. However, an important point to consider is that the company does not have a dedicated cybersecurity team or a dedicated person to handle cybersecurity aspects. This has to be considered when planning the cybersecurity strategy since it would mean that non-security experts should handle that, or experts have to be contracted.

Understand the maturity level of the business and its processes is also relevant for this initial step. The company under investigation was funded a few years ago as a startup to address issues involving the supply chain of the Pharma industry. This was initially a project within the University of Zurich but then evolve for an independent business. In 2021, the company was acquired by a Silicon Valley-based company expanding its focus on the interoperability of sensors for the supply chain of the Pharma sector and other industries, such as the construction industry. Although the current processes of the company are well-defined and the company has provided solutions for big plays in Switzerland, there is still a path to follow in order to integrate and control all of the current and the new processes, which is still a more significant challenge due to the acquisition by another company.

Based on that, it is possible to infer that the level of maturity of the company under investigation can be classified, according to the Business Process Maturity Model (BPMM) (Rosemann et al., 2004), as Repeatable (*i.e.*, Level 3 of five levels possible). Figure 4 summarizes these different levels of maturity. It is important to mention that this level of

maturity is only used as an example for the case study, as this is not a precise representation of the company processes.

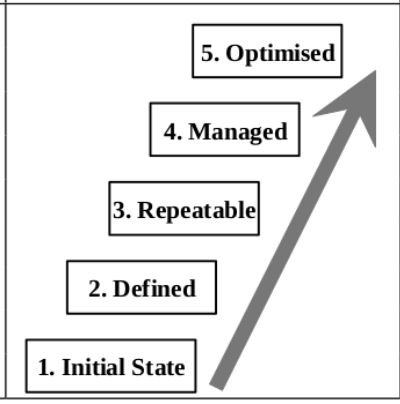
Low Maturity		High Maturity
Un-coordinated, isolated projects		Co-ordinated BPM Activities
Low BPM Skills		High BPM Expertise
Key Personnel		Organisational Wide Coverage
Reactive		Proactive
Manual		(Meaningful) Automation
Internally Focused		Extended Organisation
Low Resourcing		Efficient Resourcing
Naive		Comprehensive Understanding
Static		Innovative

Figure 4. The Business Process Maturity Model [BPMM]
Source: Rosemann et al. (2004)

Another relevant piece of information to be considered in Phase A is the history of past attacks in the company. This is an interesting metric, combined with other statistics and security trends, to help plan the cybersecurity strategy to be adopted. However, this information is very sensible and confidential for companies since malicious attackers can exploit it. Therefore, based on a literature review and the most commons attacks for the company's sector, this case study is assuming the following information a true:

- The company had a yearly average of five Phishing attacks, ten DDoS attacks, and three Malware attacks, taking into consideration the last three years of the company;
- The success rate was respectively 15% (Phishing), 20% (DDoS), and 5% (Malware), which means a percentage of these attacks impacted somehow the company (*e.g.*, economically and technically);
- Although this information clearly shows possible attack vectors, no critical impacts for the operation of its business due to cyberattacks were identified by the company in the last three years.

This kind of information can trigger alerts for the rest of the planning steps and be used as inputs for the next steps. While the company did not face any critical impact, there are high success rates for different attacks in the company. This might lead to the conclusion that this kind of attack must be carefully identified when conducting the risk assessment and the cybersecurity project definition. This can impact the company a lot in the future. For example, a phishing attack can be used as a way to infect the whole company infrastructure with a ransomware attack, which can cause business disruption, leak of data, and financial loss due to data cover. This kind of attack is increasing a lot as attackers have identified a very profitable business for this kind of illegal activity (Varonis, 2021). Therefore, the company should not rely

on the idea of no critical impacts but reads the success rate of these attacks in the business carefully.

Phase B: Threats Modeling and Security Risk Analysis

In a previous work, Hofmann (2019) conducted a threat modeling and security audit in the architecture of the BC4CC solution, which is a project with the potential to be explored in the market as a product. The author highlighted the architecture is well-defined but there is room for improvements to avoid security threats. Also, a list of potential attack vectors and its stakeholders was summarized in the work. Table 2 summarizes the most relevant threats and security issues that the company have to be aware when adopting the BC4CC solution in its portfolio.

Table 2. Overview of threats that might face the company and possible countermeasures for risk mitigation

Threat	Likelihood	Impacts	Possible Countermeasures
Misconfiguration and Outdated software	Likely	Loss of availability, introduction of common security issues.	Introduce processes for regular review of configurations and patch management.
Insufficient logging and Monitoring	Moderate	Without this kind of information it is not possible to detect incidents, counter them, nor measure the damages.	Implement a logging infrastructure, storing logs in a separate remote system to counter tampering by adversaries.
No incident recovery process	Moderate	In case of an incident, the main goal is to regain operability of the system.	Define processes for incident recovery, implement backups strategies, and training employees in case of. an incident
Denial-of-Service attack [DoS]	Moderate	Loss of availability, business disruption.	Acquisition of protections and improvements in the infrastructure.
Phishing campaign	Likely	Stealing of credentials, information loss, and can be a door for disastrous attacks, such as Ransomwares	Employments education and training, acquisition of protections.
Data Leakage	Moderate	Direct impacts on the business according to the sensibility of the information leaked (*e.g.*, advantage to competitors and penalties due to regulations) Also, Indirect impacts have to be considered, such as the loss of reputation due to the publicity of the leakage and phishing campaigns against its customers.	Continuous monitoring and logging of the systems, identify sensitive data, encryption all data, and secure all endpoints. Well-defined processes to handle with sensitive data have to be placed by the company.
Insiders and Supply-chain attacks	Moderate	Malicious employees or third-party companies that are part of the business can compromise the whole cybersecurity of the company.	Access control, good cybersecurity practices, and a well-defined cybersecurity strategy for all companies that are part of the supply-chain.
Cross-Site Request Forgery [CSRF] attack	Moderate	It is possible to create unverified user accounts, as well as performing transactions on behalf of user, thus allowing, for example, to remove the traceability of the operations occurred.	The implementation has to make sure that an operation is carried by the user on purpose. This may be achieved if for every request of the browser, in the response of the server, an additional token is returned.

Source: Elaborated by the author based on Hofmann (2019)

In the light of that information provided by the threats modeling and security analysis conducted by professionals (*i.e.*, penetration testers and others security experts), it is possible to determine what is critical and the priorities to be considered for the definition of the level of protection required. Thus, by analyzing this information, the conclusions to be taken into consideration, with a certain level of priority, during the project requirements definition are the following:

- The risk of phishing and ransomware is increasing and it becomes as one of the biggest threat for the company;
- Improvements on the software and infrastructure being used by the company have to be taken carefully in order to ensure up-to-date and well-configured systems;
- Better strategies and processes have to be defined for ensure the monitoring and logging of critical activities that can result in threats and data leakage;
- Training and education of employees have to be done focusing on the most common threats identified for the company;
- Protections have to be acquired to protect against DDoS attacks. It is suggested to consider on-demand approaches that fits in the company budget;
- Best practices of development have to be reviewed continuously in order to avoid threats like the CSRF previously identified.

Phase C: Project Requirements

After the briefing and analysis of all threats and risks, it is now required to determine the budget available for the project, the services and equipment required, additional education and training for the employees, and the definition of the new processes that have to be implanted.

First, different protections for DDoS attacks have to be mapped. Then, a list of candidates has to be selected based on the business demands and budget available. It should consider protections that offer on-demand protection against the most common types of DDoS attacks (*e.g.*, SYN Flood, ICMP flood, and UDP flood). The following protections providers were initially selected as candidates since they have a good reputation and offer the type of protection required by the company: Imperva, Verisign, Akamai, and Cloudflare. Also, besides the protections, additional bandwidth has to be contracted to make the infrastructure that hosts critical services more DDoS resistant. One additional server has to be acquired to build redundancy in critical services and databases. For protection against viruses and malware, the license of the current antivirus (*i.e.*, Bitdefender GravityZone Business Security) has to be renewed. For that, the current solution's provider has to be consulted about the prices. However, besides the investment in protections, the training and education have to cover the

most common threats using social engineering to surpass the protections available (*e.g.,* phishing for a ransomware attack).

For education and training, a list of security certifications is available on the market. However, based on the technical expertise of the employees and the whole business analyzed, it is more suitable to dedicate budget and time for basic training for all employees know how to identify, handle, and manage threats that can target the company via e-mail scams, social engineering, and others. For that, online courses have to be considered to provide the security background, and further face-to-face courses must be considered every six months for employee training. This should become a practice for the company.

Another requirement for the project is to implement a process that ensures the storage of all logs of critical activities (*e.g.*, access logs, credentials access, and database actions) for at least three years in an external and safe environment. The company already has monitors and logging solutions, which the storage of logs could be achieved by checking directly with the solution's providers the best options. Also, another process has to be defined for the company to check monthly updates for the critical software running in the company and annual updates for non-critical software. In case of updates are available, that has to be documented and updated with priority. Finally, a process has to be defined to ensure the quality of the code developed by the company and its partners. This was already started with a bug bounty program by the company in 2018. However, additional tests and training have to be done to mitigate risks due to threats introduced by the new code. The new process has to ensure that a security analysis will be done ever before the company implements a new system or feature. Table 3 summarizes all of the project requirements.

Table 3. Project requirements, constraints, and possible providers of security solutions

Requirement	Constraints	Possible providers
i) Acquisition of a Distributed Denial-of-Service [DDoS] protection	Must be on-demand and provide defenses against SYN flood, ICMP flood, and UDP flood	Imperva, Verisign, Akamai, and Cloudflare
(ii) Additional bandwidth and server to build a DDoS resistant and redundant infrastructure	If possible negotiate with the current Internet provider to avoid contract changes	Swisscom, Salt, Sunrise, and UPC
(iii) Renew the current software against viruses and malwares	The same software must be renewed due to technical and contract demands. 40 devices coverage is required.	Bitdefender
(iv) Education and Training of employees against phishing and social engineering attacks	Must have online courses contracted for basic background and face-to-face training for specific scenarios which the company might face	Coursera, Consultancy companies, and training prepared by the University of Zurich UZH
(v) Adapt the monitoring and logging processes to store all critical logs	Must be stored out of the company premises	-
(vi) Monthly updates for critical software and semiannual updates for others software	-	-
(vii) Security analysis and code review before the deployment of new features	Must consider all of the stakeholders, threats, and risks mapped for the business	Internal analysis, consultancy companies, and security experts

Source: Original results of the research

Phase D: Cost Management

As the project already has its requirements defined and possible providers, it is possible now to estimate the costs and determine how to ensure the project's economic feasibility. It is important to determine how much money has to be invested in ensuring each of the requirements. This can be achieved by applying the Gordon-Loeb Model (*cf.* eq. 2).

The Gordon-Loeb model is applied for two different scenarios: determine (a) the maximum budget for cybersecurity and (b) the maximum budget against DDoS attacks. eq. 3 presents the calculation for the scenario (a) and the eq. 4 for the scenario (b).

$$d=1{,}500{,}000 \times 0{,}51 \times 0{,}73 \quad (3)$$
$$\text{Investment} = 55{,}845 \times 0{,}37 = \text{US\$ } 20{,}662$$

$$d = 60{,}000 \times 0{,}35 \times 0{,}34 \quad (4)$$
$$\text{Investment} = 7{,}140 \times 0{,}37 = \text{US\$ } 2{,}641$$

Note that assumptions have to be made to determine the risks and success rates of attack. For that, statistics considering the average of malware attacks and DDoS were collected, including its success rate (Varonis, 2020).

The company's total revenue was determined as US$ 1.5 million, while the risk of an attack happens to be 51%, and the success rate is equal to 73%. This information is related to the worst scenario possible: ransomware attacks that succeeded in encrypting companies' data worldwide (Sophos, 2020). The DDoS investments were considered the statistics of the average of US$ 30,000 per hour of a DDoS attack and a downtime average of 2 hours. 35% of companies worldwide were targeted by a DDoS attack in which 34% of the attacks on those companies were successful (Varonis, 2020).

Based on that, it is possible to infer that not more than US$ 20,662 per year have to be invested in cybersecurity and not more than US$ 2,641 per year in DDoS protection precisely. With that information at hand, it is possible now to analyze the different requirements and estimate what is possible to do with this budget determined by the Gordon-Loeb model. Table 4 summarizes all of the costs to address all requirements as described below.

The requirement (i) needs a decision about which of the protections available are more suitable in terms of technical and economic demands. After selecting four candidate providers, the ROSI model (*cf.* eq. 3) can be applied to determine which of them is the cost-efficient protection. In order to automate this process, the tool provided by Franco et al. (2020) is used. This tool is called ProtectDDoS and allows for the definition of business demands and selects, based on the business demands and the ROSI of each solution, which is the best protection. The tool relies on the engine of MENTOR (Franco et al., 2019) for the recommendation

process. Figure 5 highlights two solutions recommended by ProtectDDoS in order of preference.

Note that not necessarily the cheaper solution is the best one. In this case, the Incapsula solution called Imperva is preferable due to its attack types covered, the deployment time in few seconds, and the minimum leasing period allowed in days. Therefore, the Imperva Incapsula solution is the best one for the company, with Verisign the second-best decision. If costs reduction is required, it is possible to choose the second option since the price can be reduced by US$ 500. However, as the Imperva Incapsula fits the budget for DDoS protection, this will be contracted. The final value is equal to US$ 2,400 for the one-year license and all support required.

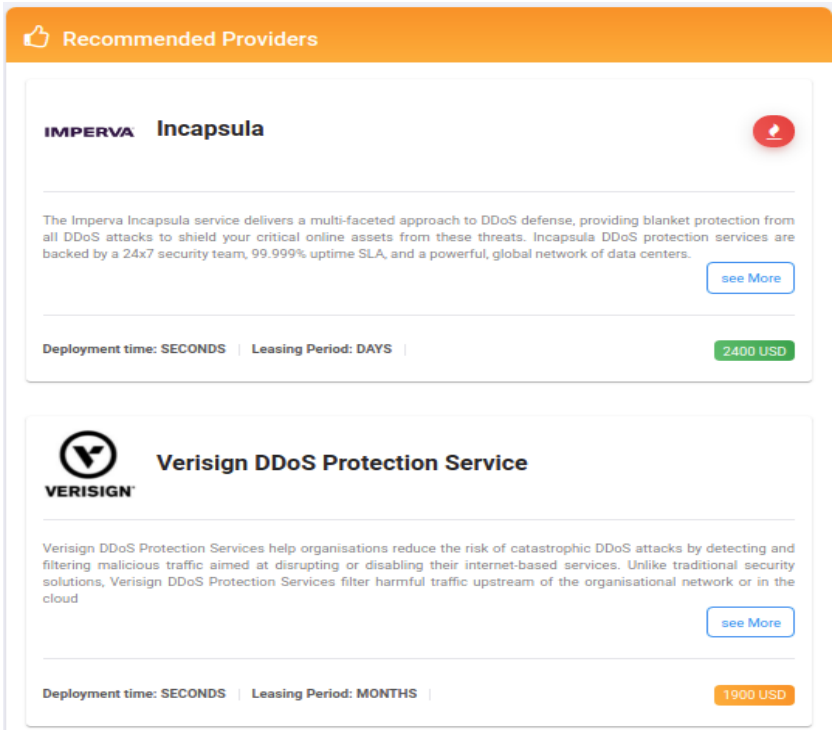


Figure 5. DDoS protection services recommended by using the ProtectDDoS tool, based on the defined company demands and the ROSI model
Source: Original results of the research

After checking with the Bitdefender provider, the GravityZone Business Security price for 40 devices coverage during three years is equal to US$ 2,600 (*i.e.*, ~US$ 850 per year). Also, Swisscom, the current Internet provider of the company, allows for an increase in the bandwidth of the network by an additional amount of US$ 100 per month (*i.e.*, US$ 1,200 per year), which also include a Failover Internet backup that allows for establishes the connection via Swisscom mobile data network in case of power failure. Therefore, the requirements (ii) and (iii*)* can be solved by using US$ 2,500 of the available budget.

For requirement *(iv)*, there are different courses available. Based on the reputation and needs, security awareness training was selected, which allows for the training of 50 employees with the investment of US$ 2,000 per year. Additionally, an on-site training conducted by the Communication Systems Group CSG of the University of Zurich is preferable since previous collaborations between the group and the company have been placed. This on-site training will cost an additional US$ 1,200 per year for the company.

The storage of logs (Requirement *(v)*) originated by the monitoring solutions can be stored on a secure cloud provided by Loggly through its SolarWinds log management service. This service allows for integrating different types of logs (*e.g.,* Linux system logs, HTTP events in the endpoints, and database access). Also, it enables a fast search to find misbehaviors. The price for this solution is US$ 159 per month in its Pro version recommended for growing companies. Thus, US$ 1,908 has to be allocated if possible for this tool. Cheaper solutions are possible but would require additional time and expertise for the usage and deployment.

The requirement (vi) stands for the continuous update and upgrade of the software and operating systems being used inside the company. Different costs have to be considered for this step, including the cost of new software licenses, additional hardware to run new software, and allocation of people to conduct the updates. For the software licenses and hardware updates, it is reasonable to allocate around US$ 1,000 per year. As most of the software running inside the company is developed for specific purposes or is open-source, it is not expected to have too many costs with licenses in the next few years. Therefore, the most significant part of this reserved amount can be used to replace hardware that impacts the company's security. Also, one employee must be responsible for this activity, assuming that the company already has this employee on its board. Therefore, no additional costs for personnel for the introduction of this new process.

Finally, the requirement *(*vii*)* involves defining a new process that involves the security analysis and audit of code when a new feature or system is implemented. For that, on-demand consultancy can be contracted, or a dedicated team can be contracted for that activity. As the company has to think more about its core business and cannot allocate too much personnel for security analysis and audit, it is recommended to contract a consultancy company when required. An example, PwC Switzerland, a famous consultancy company, has a Cybersecurity as a Service [CaaS] model that can be used when a new element has to be checked. However, it is preferred to contract a security expert who knows the company architecture and continuously checks for vulnerabilities when requested. This security expert will cost an average of US$ 5,000 per year based on an average of five new critical features analyzed per year.

Thus, as summarized in the Table 4, after the calculations, the cost to implement this cybersecurity strategy in the company is US$ 15,558. This amount fits the budget previously defined as the maximum investment (*i.e.*, US$ 20,662). Therefore, an amount of roughly US$ 5,000 can still be used to address any issue along with the execution of the project, such as contract experts for specific tasks or unexpected changes in the cost of solutions previously identified.

Table 4. Summary of all costs mapped to achieve the requirements of the project in terms of level of security

Investment	Requirement Covered	Cost (yearly)
Protection against Distributed Denial-of-Service [DDoS]	(i)	US$ 2,400
Antivirus and Malware	(ii)	US$ 850
More bandwidth and resistant against DDoS	(iii)	US$ 1,200
Online security awareness education and on-site training	(v)	US$ 3,200
Storage and management of critical logs	(vi)	US$ 1,908
Continuous update and upgrade of software	(vii)	US$ 1,000
Security analysis and code verification	(vii)	US$ 5,000
-	Total	US$ 15,558

Source: Original results of the research

Phase E: 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 the project execution. Table 5 summarizes the risks identified to the cybersecurity project affected by time, costs, and performance.

Table 5. 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 required for the supply chain	Minor	Unlikely	Low

Source: Original results of the research

As shown in the last column, 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. Therefore, the risks related to the management can be mitigated by using more budget in case of needs. Also, this budget can be allocated to address the issue of lack of in-house expertise for manage the project, such as for the training of a selected employee or for the payment of externals (*e.g.*, consultants or freelancers) to handle this activity.

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.

Phase F: Execution and Deployment

Finally, the last step of the SECProject framework involves the execution of the project and deployment of the cybersecurity strategy, taking into account all information and requirements defined in the previous steps. For that, technical support, if not placed in the company already, can be achieved by consultants. Also, a clear deployment schedule has to be defined since some sectors of the company might need to stop their operations for a few hours to have the full deployment of the solutions. Also, the schedule for the whole project has to be clear at this step of the project.

Note that after the deployment of the cybersecurity, operation, and maintenance tasks are continuous and have to follow all requirements defined for the project. These tasks have to be covered by the budget, technical expertise, and new processes implemented by the company. In this case study, these operation and maintenance tasks involve the continuous monitoring of critical activities, the update of software, and maintenance of the solutions implemented for protection (*i.e.*, ensure that all is working according to the needs).

Thus, after following in detail all of the steps provided by the SECProject framework, the studied company was able to (a) define its cybersecurity demands, (b) determine the threats, (c) describe the requirements to achieve an adequate level of protection according to its needs, (d) understand and plan the costs of implementing such kind of cybersecurity measures, (e) identify the risks of problems that might impact the execution of the project, and, finally, (f) execute and deploy the project. After the deployment, the company is expected to

achieve the right level of protection according to the demands to explore its new product called BC4CC in the market, without putting in critical risks its assets, reputation, and profits.

Conclusion

This work proposed a six steps framework for the planning, definition, and execution of a cybersecurity project for SMEs. It is supposed that 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, such as threat modeling to identify the requirements for better cybersecurity, cybersecurity economics models for optimum investments, and risk management to understand and reduce the chances of failures during the project execution.

In conclusion, there is still room for novel frameworks and tools to help for 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, suppose all required information can be achieved. In that case, the SECProject 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. At the same time, some steps also can be reduced or extended to achieve the overall goal of implementing a cybersecurity strategy. Therefore, additional steps can be considered, or different project management techniques can be integrated within the SECProject's steps to achieve a better and accurate project in terms of costs, risks, and technical aspects.

As future work, it is suggested (a) the design and development of a visual tool to support the calculations of the costs of the project, which can be based on the cybersecurity economic models discussed along with the work, (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. Also, additional case studies and interviews can be conducted with selected partners to refine the framework according to real-world demands.

Acknowledgements

The author would like to thank the Communication Systems Group CSG of the University of Zurich for providing the resources and relevant information for conduct this work, specially the case study. Also, I would like to thank Dr. Fabricio Lacerda for his supervision and insightful reviews along with this work. Last but not least, I would like to thank my family and friends for their unconditional support in all of my life and work projects.

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.

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 2021.

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

Eisenhardt, K. 1989. Building Theories from Case Study Research. The Academy of Management Review. Vol. 14, No. 4: 1-19.

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

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

Franco, M.; Rodrigues, B.; Scheid, E.; Jacobs, A.; Killer, C.; Granville, L.; Stiller, B. 2020. SecBot: a Business-Driven Conversational Agent for Cybersecurity Planning and Management. In: 16th International Conference on Network and Service Management (CNSM), Izmir, Turkey, October 2020, p. 1-8.

Franco, M.; Rodrigues, B.; Parangi, G.; Stiller, B. 2019. Cybersecurity Threats, Stakeholders, and SEConomy Framework – An Economic Analysis for Cybersecurity. CONCORDIA H2020 Project T4.3. Initial Report, Zurich, Switzerland, Available at <https://files.ifi.uzh.ch/CSG/staff/franco/extern/publications/Report-on-Economics-Perspectives.pdf>. Accessed on: December 9 2021.

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.

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. Available at < https://files.ifi.uzh.ch/CSG/staff/scheid/extern/theses/IS-A-Hoffman.pdf>. Accessed on: August 3 2021.

Ishikawa, K. 1976. Guide to Quality Control. Industrial Engineering and Technology, Asian Productivity Organization, Tokyo, Japan.

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.

Liu, L.; De Vel, O.; Han, Q.; Zhangm, J.; Xiang, Y. 2018. Detecting and Preventing Cyber Insider Threats: A Survey. IEEE Communications Surveys & Tutorials 2: 1390-1417.

Modum AG. 2017. Data Integrity for Supply Chain Operations, Powered by Blockchain Technology. Whitepaper Version 1.0. Available at <https://assets.modum.io/wp-content/uploads/2017/08/modum-whitepaper-v.-1.0.pdf>. Accessed on: 18 June 2021.

National Institute of Standards and Technology (NIST). 2018. Framework for Improving Critical Infrastructure Cybersecurity. Available at < https://doi.org/10.6028/NIST.CSWP.04162018>. Accessed on: 20 April, 2021.

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.

Rosemann, M.; de Bruin, T.; Hueffner, T. 2004. A Model for Business Process Management Maturity. In: 15th ACIS. Association for Information Systems, Hobart, Australia, p. 1-6.

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.

Scheid, E.; Rodrigues, B.; Killer, C.; Franco, M.; Niya, S.; Stiller, B. 2021. Blockchains and Distributed Ledgers Uncovered: Clarifications, Achievements, and Open Issues. Advancing Research in Information and Communication Technology, Springer, Cham, Switzerland, No. 1: 1-29.

Schmit, J. T.; Roth, K. 1990. Cost Effectiveness of Risk Management Practices. Journal of Risk and Insurance: 455-470.

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.

Sophos. 2020. The State of Ransomware 2020. Whitepaper. Available at < https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf>. Accessed on: August 9 2021.

Stiller, B.; Rodrigues, B.; Scheid, E.; Parangi, G. 2020. Blockchains for Coldchains (BC4CC). Final Technical Report. Available at <https://files.ifi.uzh.ch/CSG/staff/scheid/extern/publications/BC4CC-Final-Report-v4.pdf>. Accessed on: 18 June 2021.

Varonis. 2021. 134 Cybersecurity Statistics and Trends for 2021. Available at < https://www.varonis.com/blog/cybersecurity-statistics/>. Accessed on: August 9 2021.

Wanner, R. 2015. Project Risk Management - Practical Guide. 2nd Edition. Amazon Distribution.