X SINGEP
Simpósio Internacional de Gestão, Projetos, Inovação e Sustentabilidade
International Symposium on Management, Project, Innovation and Sustainability
ISSN: 2317-8302
CYRUS Institute of Knowledge MAKE A DIFFERENCE
CIK 10th INTERNATIONAL CONFERENCE

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

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

MURIEL FIGUEREDO FRANCO
USP - UNIVERSIDADE DE SÃO PAULO

FABRICIO MARTINS LACERDA
UNIVERSIDADE ESTADUAL DO PARANÁ - UNESPAR - CAMPUS APUCARANA

BURKHARD STILLER
UNIVERSITY OF ZURICH UZH

Nota de esclarecimento:
O X SINGEP e a 10ª Conferência Internacional do CIK (CYRUS Institute of Knowledge) foram realizados de forma remota, nos dias 26, 27 e 28 de outubro de 2022.

Agradecimento à orgão de fomento:
This paper was supported partially by (a) the University of Zurich UZH, Switzerland and (b) the European Union's Horizon 2020 Research and Innovation Program under Grant Agreement No. 830927, the CONCORDIA project.

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

Objetivo do estudo
Compreender e organizar os diferentes passos e informações necessárias para implementar uma estratégia adequada de cibersegurança, considerando diferente conceitos de gerenciamento de projetos para que o planejamento e execução da implantação de novas proteções ocorra conforme os requisitos e necessidades das empresas.

Relevância/originalidade
Uma abordagem multidisciplinar baseada nos diferentes passos e informações necessárias para simplificar e agilizar a adoção de estratégias de cibersegurança ao mesmo tempo que otimiza a utilização de recursos durante o planejamento e execução de projetos para implantação de novas proteções.

Metodologia/abordagem
Mapeamento dos processos, stakeholders e informações críticas para definição de estratégias de cibersegurança, seguido de uma investigação da literatura de abordagens de gerenciamento de projetos para cibersegurança Após, considerando todos os elementos mapeados, o framework SECProject é proposto e avaliado.

Principais resultados
Como principal resultado é apresentado o framework SECProject, que, apoiado por conceitos-chave de gestão de projetos, define os passos e informações necessárias para o planejamento e implementação de uma estratégia de cibersegurança em uma empresa. Aspectos ecônomicos da cibersergurança também são considerados.

Contribuições teóricas/metodológicas
Mapeamento de todas as etapas necessárias para definição de requisitos, análise de ameaças, gerenciamento de custos, gerenciamento de riscos e execução de um projeto para implementação de estratégias de cibersegurança em PMEs. Todos os passos e informações são detalhadas no trabalho.

Contribuições sociais/para a gestão
O framework proposto permite a utilização de técnicas de gerenciamento de projetos e cibersegurança mesmo em empresas sem conhecimentos técnicos especializados, de modo a permitir a definição e execução de um projeto que resulte em uma melhor estratégia de cibersegurança.

Palavras-chave: Cibersegurança, Gerenciamento de Riscos, Gerenciamento de Custos, Gerenciamento de Projetos, Aspectos Ecônomicos da Cibersegurança

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

Study purpose
Understand and organize the different steps and information required to implement a proper cybersecurity strategy, thus, considering the different concepts of the project management field to plan and execute the deployment of new protections according to the demands and requirements of companies.

Relevance / originality
A multidisciplinary approach based on the main steps and information required to simplify the adoption of cybersecurity strategies while optimizing the time and resource usage during the planning and execution of projects to deploy new protections in a company.

Methodology / approach
Mapping of the processes, stakeholders, and critical information for the definition of cybersecurity strategies, followed by a literature review of approaches exploring project management in cybersecurity. Next, the SECProject framework is proposed and evaluated by taking all mapped elements into account.

Main results
The SECProject framework is presented as the main result. The framework, supported by key project management concepts, defines the steps and information required for planning and deploying cybersecurity strategies in companies. Also, the economic aspects of cybersecurity are investigated and considered.

Theoretical / methodological contributions
Mapping all steps for the definition of the project requirements, threat analysis, cost management, risk management, and execution of a project for the deployment of cybersecurity strategies in SMEs. The relevant steps and information are detailed and considered in the SECProject framework.

Social / management contributions
Mapping the steps for defining the project requirements, threat analysis, cost management, risk management, and execution of a project for deploying cybersecurity strategies in SMEs. Using the SECProject, companies without technical expertise can reduce their business risks and optimize their investments.

Keywords: Cybersecurity, Risk Management, Cost Management, Project Management, Cybersecurity Economics

1 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 (Franco et al., 2022).

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 wrong 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. 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 approaches 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 phases, 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 phases: (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 introduced in details in this work. Also, a practical application of the SECProject 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 the 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 evaluation 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.

The remainder of this work is organized as follows. Section 2 describes the methodology, paths investigated, and tools used during the development of this work. Also, all steps and decisions taken for the development of the proposed framework are presented in a proper level of details. Then, the SECProject framework is introduced in Section 4, followed by an overview of the case study conducted. Finally, Section 5 concludes the work providing the final remarks and giving insights on future work.

2 Background and Related Work

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 and 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 apply up- or re-skilling 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.

Figure 1 lists examples of different type of incentivies 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. The fines for violating the GDPR are substantial, with a maximum of € 20 million or 4% of a company's global revenue (the higher value of those is considered). 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.

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
Cybersecurity Canvas	Methodology	SMEs

Figure 1. Examples of Initiatives for Cybersecurity Regulations, Organizational Guidelines, and Threat Modeling Approaches
Source: Original data of the research

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). 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 and 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. Similarly, DREAD is used for assessing threats and stands as a mnemonic for Damage potential, Reproducibility, Exploitability, Affected Users, and Discoverability. Currently, there are also 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: (i) Preparation and Assessment, (ii) Management Level, (iii) Technical Level, (iv) Attacks Management, and (v) Implementation and Improvement. The framework defines eleven obligatory tasks (e.g., objectives of security and budget, definition of critical systems, and employee awareness-raising) for all organizations, ten strongly recommended but not mandatory, and four recommended but optional. 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, 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.

3 Methodology

There are two main challenges considered in this 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 address these challenges, 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.

Thus, the development of this work focuses on the processes, tasks, and information required for the design of a framework for assessment and management of cybersecurity projects. 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.

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). 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 estimation 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 as result of this work, with all its inputs, processes, and outputs described in detail. 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.

Therefore, the evaluation of the framework relied on a 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 blockchains (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 US$ 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, Switzerland. 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).

Figure 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 in each phase, 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).

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.
Portfolio	Monitoring Sensors and Full-Fledged Platform for Supply Tracking	This information gives an overview of the products and it is important for the risk analysis and threat modeling tasks.

Figure 2. Example of Information of a Company Being Considered as Input for the SECProject
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.

Based on this business profile, the SECProject can be applied, for example, by 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 results section, is applied.

All of the information required for the validation of the SECProject 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.

4 Results

This section presents the different contributions of this work and highlights 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 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.

4.1 Overview of the SECProject Framework

Figure 3 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, including 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.

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:

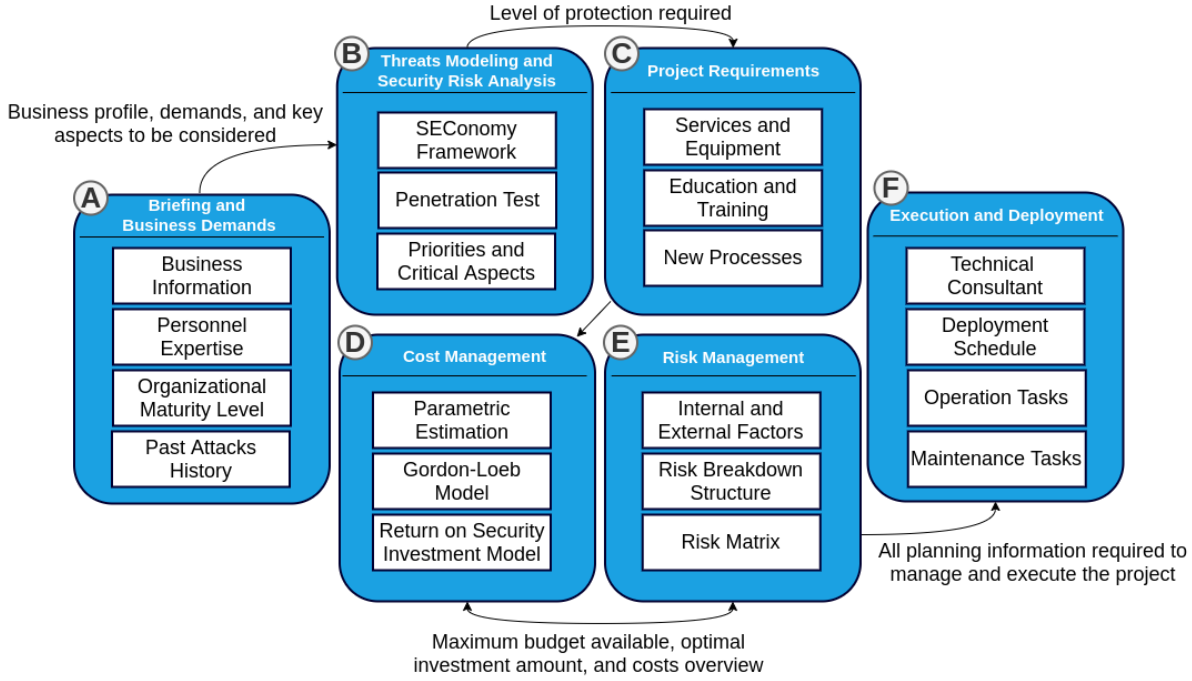

Figure 3. Overview of the SECProject Framework
Source: Original results of the research

- 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 Equation 1.

$$E_{Parametric} = \frac{A_{old}}{P_{old} \times P_{curr}}$$

Equation 1: Parametric Estimating Formula
Note: 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*). Equation 2 describes how to use this information for the calculation.

$$\text{Investment} = d \times 0.37$$

Equation 2: Maximum investment calculated using the Gordon-Loeb model
Note: $d = \lambda \times t \times vg$
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, or 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.

With the protection solutions mapped, the next phase consists of the analysis of the ROSI for each one of the solutions and strategies mapped to be deployed. 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 Equation 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 (*i.e.*, 100% of payback).

$$\text{ROSI} = \frac{\left((\text{ALE} \times \text{Mitigation Rate}) - \text{Cost of the Investment}\right)}{\text{Cost of the Investment}}$$

Equation 3: General Calculation of the ROSI
Note: $\text{ALE} = \text{SLE} \times \text{ARO}$
Source: Sonnenreich et al. (2005)

The ROSI uses the Annual Loss Exposure (ALE), the mitigation rate, and the cost of the investment to assess whether 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.

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 make adjustments to achieve not only cost-effective cybersecurity but a feasible project to be implanted and operated by the 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, 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 show 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.

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, this phase of the SECProject focuses on evaluating the risks of implementing a cybersecurity project, not the cyber threats itself. 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 a low risk and it is easily mitigated by well-defined processes, while a critical impact has mostly very high risks and might require abandoning the project.

Figure 4 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 an issue 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 must be taken.

Likelihood \ 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)
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 4. 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 cybersecurity 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 phase in order to have not only proper 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.

4.2 Case Study

For the evaluation of the SECProject, a case study considering an SME that provides innovative solutions for the supply-chain tracing in the Swiss pharma industry is considered. All of the steps defined by the SECProject framework were applied to reduce project risks and deploy an adequate cybersecurity strategy. The first phase consisted of using the information available in Table 1 as input for understanding the company (*i.e.*, Briefing and Demands). Next, the threat modeling and security audit of the architecture of the BC4CC solution was conducted. This analysis was based on previous work done by Hofmann (2019). Eight main threats were identified, which Software Misconfiguration and Phishing Campaigns being those threats with higher likelihood and risk.

Next, Phase C started with defining project requirements (*i.e.*, cybersecurity demands). Figure 5 highlights the seven requirements defined to address all demands and reduce the risks mapped in the phase before. Examples of requirements include: the acquisition of protections against DDoS, education and training of employees regarding phishing attacks, monthly updates for critical software, and security analysis and code review before deploying new features in the company's software. Also, possible providers to address each one of the requirements were listed in this phase.

Requirement	Constraints	Possible providers
i) Acquisition of a 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

Figure 5. Project Requirements, Constraints, and Possible Providers of Security Solutions
Source: Original results of the research

Phase D focuses on optimizing the project's costs based on the available budget. The Gordon-Loeb model was used, as shown in Equation 4, to calculate the maximum investment, equal to US$ 20,662, considering all threats and requirements mapping.

For such a calculation, 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).

$$d = 1{,}500{,}000\ x\ 0{,}51\ x\ 0{,}73$$

Investment = 55,845 x 0,37 = US$ 20,662

Equation 4. The Maximum Budget to invest in Cybersecurity Calculated using the Gordon-Loeb model
Source: Original Results from the Research

Figure 6 shows the costs mapped to achieve the requirements of the Project. These costs are calculated by analyzing the market and selecting the best solutions to address each requirement, the project's total cost (software, hardware, and new processes added) is equal to US$ 15,558. This amount fits the budget previously defined as the maximum investment (i.e., US$ 20,662). Therefore, 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. Note that this is the maximum amount but not the optimal amount. The optimal amount to invest in cybersecurity can also be calculated using the Gordon-Loeb model (Gordon and Loeb, 2021) and additional information. However, this is out of the scope of this work.

Investment	Requirement Covered	Cost (yearly)
Protection against 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**

Figure 6. Summary of All Costs Mapped to Achieve the Requirements of the Project
Source: Original Results from the Research

The management of the project is done continuously in Phase E. Four types of risks were considered for the execution of the project, which include technical, management, external, and commercial risks. Figure 7 highlights the risks identified to the cybersecurity project affected by time, costs, and performance. As can be seen, some overall risks are considered very high to 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 LGPD 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.

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

Figure 7. List of Risks for the Execution of Project
Source: Original Results from the Research

Finally, the last phase of the SECProject framework involves executing the project and deploying the cybersecurity strategy, taking into account all information and requirements defined in the previous phases. For that, technical support can be achieved by contracting specialized consultancy if not placed in the company already. 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 deploy the protections fully. Also, the schedule for the entire project has to be clear at this phase of the project.

Note that after the deployment of the cybersecurity, the operation and maintenance tasks are continuous and have to follow all requirements defined for the project. These tasks must 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 the maintenance of the protection solutions implemented (*i.e.*, ensuring that all is working according to the requirements).

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 proper level of protection according to the demands to explore its new product (*i.e.*, BC4CC) in the market without putting critical risks to its assets, reputation, and profits. Note that this case study considers all information as close as possible to the real-world, with assumptions when information is missing. Also, this case study only highlights all phases needed using the studied company as an example to prove the feasibility of the SECProject framework, but not actually implementing any measure on the existing company infrastructure.

5 Conclusions

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 affect both small, medium, and multinational companies worldwide. For that, the SECProject framework explores concepts of the project management field to organize 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 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 are still required when applying frameworks like the 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.

During the application of the SECProject, 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 more accurate project in terms of costs, risks, and technical aspects.

There are also limitations of the work to be considered. First, the framework is not exhaustive in the aspects covered. Therefore, additional phases or steps might be needed for specific scenarios. However, this can be used as an initial guideline to determine such elements. Secondly, the evaluation relies only on a case study considering a single company. Although it provides evidence of the feasibility of the framework, more in-depth investigations are needed in companies with different characteristics, and more real-world scenarios are needed.

In 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 coverage 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.

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 2022.

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

European Watch on Cybersecurity & Privacy. (2021). Cybersecurity Label. Available at <https://label.cyberwatching.eu/>. Accessed on: August 2, 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.

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

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.; 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. F.; Sula, E.; Huertas, A.; Scheid, E. J.; 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.

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, 2022.

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, 2022.

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, 2022.

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: 20 April, 2022.

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.

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.

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.

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 2, 2022.

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 2022.

Varonis. (2021). 134 Cybersecurity Statistics and Trends for 2021. Available at <https://www.varonis.com/blog/cybersecurity-statistics/>. Accessed on: August 2, 2022.

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 (CSR 2022), IEEE, Virtual Conference, p. 1-8.

Xiong, W.; Lagerstrom, R. (2019). Threat Modeling – A Systematic Literature Review. Computer & Security: 53-29.

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