CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment

Muriel Figueredo Franco[1], Lisandro Zambenedetti Granville[2], Burkhard Stiller[1]
[1]*Communication Systems Group CSG, Department of Informatics IfI, University of Zürich UZH*
Binzmühlestrasse 14, CH—8050 Zürich, Switzerland
[2]*Computer Networks Group, Institute of Informatics, Federal University of Rio Grande do Sul UFRGS*
Av. Bento Gonçalves, 9500, Porto Alegre, Brazil
E-mail: [franco, stiller]@ifi.uzh.ch[1], granville@inf.ufrgs.br[2]

***Abstract*—It is essential to look at cybersecurity not only as a technical problem but also from economic, societal, and legal perspectives. Companies need to pay more attention to planning and investments in cybersecurity due to different factors, such as budget constraints and complexities involved in the planning and decision-making processes. Also, companies wrongly do not see themselves as the target of a potential cyberattack. Therefore, there is still a need for approaches that support companies, especially Small and Medium-sized Enterprises (SME), during the cybersecurity planning and investment decisions.**

This PhD thesis addressed cybersecurity planning and investment gaps by proposing the CyberTEA approach. This approach is composed of a five-phase methodology, a framework, and a set of solutions for cybersecurity planning and investment, considering the technical requirements of cybersecurity and its economic dimensions, such as the potential economic impacts of cyberattacks and the cost-benefit of protections available on the market to protect against specific threats. The evaluations and scientific advances of CyberTEA approach was proven valid to support SMEs while also showing the benefits and opportunities for cybersecurity economic approaches.

I. Introduction

The increasing number of cyberattacks and their potential disruptive impacts cause significant concerns for companies, governments, and society. A successful cyberattack can, for example, cause financial losses due to business disruption, affect the privacy of people due to data leakages, and make critical resources completely inaccessible for interested stakeholders. This puts cybersecurity at the center of a digital society and as one of the anchors to all technologies and industries that support a connected and automated society. Therefore, it is essential to look at cybersecurity not only as a technical problem but also from the economic, societal, and legal perspectives.

Today, companies still neglect planning and investments in cybersecurity due to different factors [1]. First, they face budget constraints and do not see cybersecurity investments as a priority. Secondly, the high amount of information and planning complexities makes implementing a cybersecurity strategy cumbersome for companies that do not have in-house expertise. Finally, companies, especially Small and Medium-sized Enterprises (SME), do not see themselves as the target of a potential cyberattack. This utterly wrong view makes SMEs one of the main targets of cyberattacks worldwide since the likelihood of successful cyberattacks is higher than companies with a well-defined cybersecurity strategy. Therefore, there is still a need for approaches that support companies during the cybersecurity planning and investment phases. These phases include supporting the understanding and definition of cybersecurity requirements, the definition of the budget and investment path to achieve a proper level of cybersecurity, and the selection of protections with a positive return on investment, while also satisfying specific business demands.

This PhD thesis addressed these gaps in cybersecurity planning and investments by proposing the Cybersecurity Technical and Economic Approach (CyberTEA) [7]. It covers security management from a business-oriented perspective. The CyberTEA approach comprises a five-phase methodology, a framework, and a set of solutions for cybersecurity planning and investment, considering the technical requirements of cybersecurity and its economic dimensions. The methodology describes the key phases to consider during the cybersecurity planning and investment, while the framework maps and implements the components needed to be considered to support the tasks required in each phase. A set of novel solutions, supported by information visualization technologies and economic theory methods, are also designed and implemented to *(a)* simplify the risk assessment of companies, *(b)* analyze and classify cyberattacks, *(c)* calculate the optimal investment in cybersecurity, and *(d)* recommend protections based on businesses profile.

Quantitative and qualitative evaluations were conducted to analyze different aspects that give evidence of the feasibility, accuracy, and performance of the proposed solutions. The results highlight the potential of using the *CyberTEA* approach for effectively planning cybersecurity strategies. This also includes the benefits of applying the developed solutions in different mapped planning and investment phases to achieve simplified and better cybersecurity, even for companies without in-house expertise.

The remainder of this paper is organized as follows. Section II introduces the research questions and highlights the key contributions of this work. Section III introduces *CyberTEA* approach, while Section IV contains the evaluation, followed by conclusions and future work in Section V. Section VI presents final remarks regarding this PhD thesis.

II. Research Questions and Contributions

This PhD thesis tackled identified cybersecurity planning and investment challenges by providing an approach that addresses the relevant steps, from a technical and economic view, required for the planning and implementation of an efficient cybersecurity strategy, thus, supporting companies with technical and economic constraints to achieve a suitable level of protection for their information and systems. Within this context, five Research Questions (RQ) were defined to guide the research conducted in this PhD thesis. Thus, it is driven by the following RQs:

RQ1 - Which technical and economic aspects have to be considered during the planning and investing process to adopt cybersecurity strategies in SMEs?

This RQ1 involves the analysis of the different requirements to be considered before decisions to invest in a specific cybersecurity measure. The work on RQ1 will assess the current SME scenarios, considering their requirements. A deep understanding about the market, its cybersecurity culture, and main threats is required to map the most important steps of the cybersecurity planning in SMEs.

RQ2 - What are and how to organize and simplify the key steps, information, models, and techniques required for an effective definition of a cybersecurity strategy in SMEs?

This RQ2 focuses on mapping and selecting the essential steps into phases to guide the SME to plan and define a cybersecurity strategy. The inputs from RQ1 have to be used to provide a methodology that supports SMEs to address all the different requirements, steps, and challenges involved in cybersecurity planning and investment.

RQ3 - What are the necessary architectural components and actors to satisfy key steps and to allow SMEs to implement cost-effective cybersecurity strategies?

This RQ3 focuses on the challenge of determining how to integrate different cybersecurity planning solutions in a framework with a well-defined flow, components, and actors. This integration also has to consider the different information that has to be processed by specific components to be used as input for the different solutions. Thus, this RQ3 determines a technical path to be followed by the solutions proposed to answer the RQ5.

RQ4 - How to determine the optimum amount of resources (*e.g.*, money, personnel, and time) an SME should invest in cybersecurity based on their specific technical and economic demands?

This RQ4 consists of the analysis of the trade-offs between investments and protection. This RQ focuses on investigating the amount of money and the level of protection appropriate for a cost-effective cybersecurity strategy. Thus, the focus is on understanding whether there is a maximum or minimum budget for cybersecurity in SMEs (*e.g.*, based on the company's yearly revenue). Also, from an economic perspective, it is important to understand whether known risks can be assumed or shared, instead of investing more money in cybersecurity.

RQ5 - How to provide cybersecurity solutions capable of abstracting technical details to guide SMEs during the plan and execution of a cybersecurity strategy?

This RQ5 focuses on the proposal of solutions sustained by proof-of-concepts implementations to show the benefits for SMEs and the feasibility of these solutions, focusing on supporting SMEs' adoption of better cybersecurity strategies. The proposed solutions have to fulfill the different elements identified in RQ1, RQ2, and RQ3.

In order to answer these RQs listed above, three major aspects had to be considered and investigated during the research, design, and development of this PhD: *(a)* the critical steps and information for conducting cybersecurity planning and investment, *(b)* the technical and economic requirements for a feasible cybersecurity strategy, and *(c)* the features required for solutions to address the current gaps of SMEs during the process of protecting their business.

This PhD thesis provides contributions to the advancement of the state-of-the-art in the cybersecurity and security management, most specifically those challenges related to cybersecurity planning and investments. These contributions are summarized as follows:

- **A methodology with well-defined steps to guide SMEs in the process of cybersecurity planning and investments.** A methodology is proposed with the technical and economic key steps mapped for SMEs to conduct cybersecurity planning and investments, including the information and complexities related to risk assessment, definition of technical requirements, cost management, and deployment of cybersecurity strategies.
- **A framework to address SMEs challenges using different solutions.** A technical framework is designed to address the steps determined by the methodology, thus, highlighting all different stakeholders, components, and interactions required to achieve an ecosystem that covers and supports the most relevant cybersecurity planning and investments processes.
- **Novel solutions to support the decision-making processes of SMEs toward a better cybersecurity strategy:** the design of architectures and development of novel and refreshed cost-efficient solutions are done to provide features that implement core components of the proposed framework that fulfills key steps mapped by the defined methodology. Examples of these solutions include a protections recommendation system, a conversational agent for cybersecurity management, intuitive risk assessment tools based on companies' configuration and specific sectors, threat identification based on the visualization of network traffic, and decentralized cyber insurance models.

Figure 1 summarizes the these contributions by highlighting the different pieces of work (*i.e.*, methodology, framework, and solutions), from the more general to a more specific level, that compose the CyberTEA. These contributions improve the understanding of SMEs' cybersecurity planning and investment processes, such as the definition of business profiles,

demands, and key aspects to consider during the planning and deployment of a cybersecurity strategy. Further, providing a framework that allows for the integration and simplification of the different cybersecurity steps involved. Finally, novel solutions (*i.e.*, systems and tools) can support the decision process for planning and investing in cybersecurity while also reduces the complexities of understanding businesses risks and cyberattack behavior.

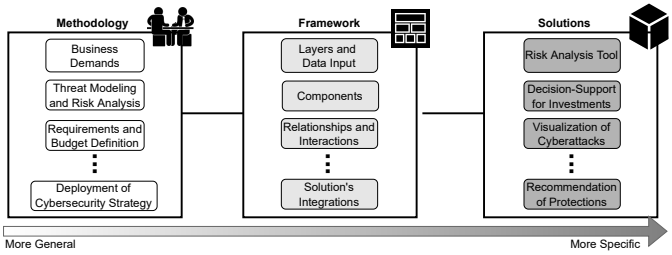

Fig. 1: Overview Contributions of This PhD thesis

III. The *CyberTEA* Approach

Determining stakeholders and their economic dimension concerning the costs of different systems and processes is one important pillar for efficient cybersecurity planning. Besides, there are different steps to be followed to plan and deploy an effective cybersecurity strategy not only from a technical perspective but also considering economic aspects (*e.g.*, cyberattack costs vs. protection costs). For that, the CyberTEA [7] focuses on three main contributions: *(a)* a methodology that maps key elements and guides business in the initial and critical steps when planning a cybersecurity strategy, *(b)* a framework that defines the components required to be implemented by solutions that aim to cover the important steps of cybersecurity planning, and *(c)* a set of solutions that implements different features to support the planning, investments, and deployment of cybersecurity. Besides satisfying components determined by the framework proposed, these solutions can be mapped within the methodology defined by the *CyberTEA* approach.

A. Defined Methodology for Cybersecurity Planning

The proposed methodology comprises five phases representing sequential tasks decision-makers must consider, when planning a new (or updating an already placed) cybersecurity strategy. Examples of the definition of cybersecurity strategies, defined using CyberTEA in the background, are highlighted in [10], [13]. Figure 2 shows the methodology, including all phases (from A to E) and examples of critical steps that must be performed in each one of these phases. This methodology was defined based on an in-depth literature review, interviews with cybersecurity experts and decision-makers from industry, SMEs, and academia, and based on all knowledge obtained and discussions conducted. It is important to mention that the steps highlighted for each phase are not exhaustively listed; thus, they are general steps common for most companies but not a final list. The methodology can be extended and adapted to fit the specific demands of a particular company or sector.

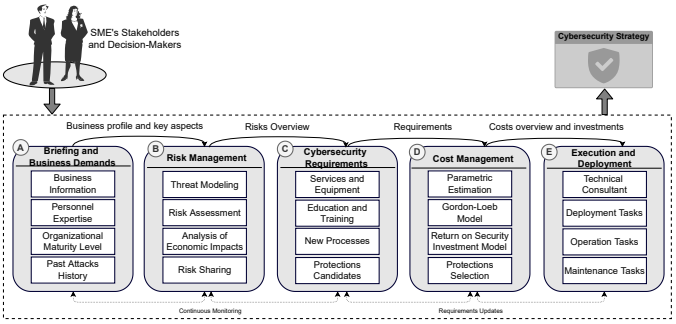

Fig. 2: The Methodology for Cybersecurity Planning and Investment with the Five Phases Mapped by the *CyberTEA*

This methodology shows a path for companies to start planning and investing in cybersecurity. However, many of these steps are not trivial, since most SMEs do not have this amount of information or solutions to support them in all of these steps. In order to address this issue, a framework architecture has been proposed to describe the main different layers and components required to be implemented by solutions that want to support these relevant steps in an integrated, simplified, and effective way. It is worth noting that cybersecurity strategies may vary from company to company, along with the available budgets. Therefore, the methodology can be used as a guideline for the critical phases to be performed during the planning. However, the steps of each phase are not exhaustively listed; therefore, it cannot be seen as a one-size-fit approach since it might change based on the reality of the company.

B. Proposed Technical Framework

The framework is an important contribution provided by the *CyberTEA* approach to help decision-makers and software developers understand the requirements, information, and relationships between components, when developing cybersecurity planning and investment solutions. Also, the framework maps essential components analyzed, designed, and implemented by the *CyberTEA* to provide data, information, and elements that enable companies to perform all steps defined in the methodology explained before (*cf.* Figure 2). It is worth mentioning that the framework is not exhaustive and is defined to be modular. This modular architecture allows for integrating solutions already placed in the real-world and those under research once a company or a specific model can require additional steps or information. Therefore, the framework maps and implements all methodology phases into layers and components while providing a concise path for emerging novel solutions to support cybersecurity planning and investments.

The framework, proposed as part of the *CyberTEA* approach, is divided into four layers, as shown in Figure 3. The **Business Layer (BL)** represents the interface between the user and the different components, also being in charge

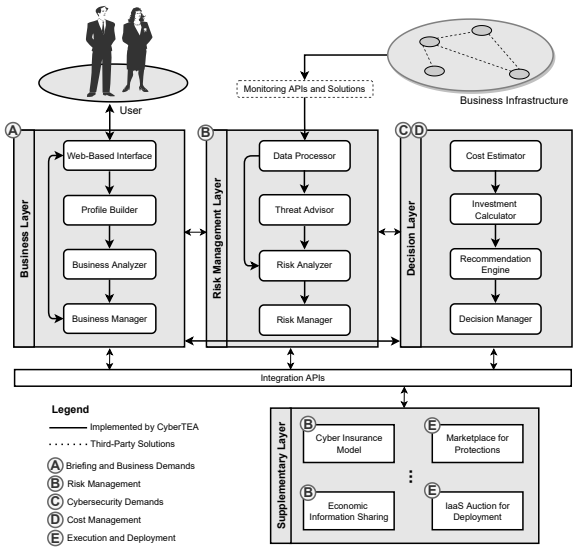

Fig. 3: The Architecture of the Framework Defined by the *CyberTEA* Approach

of receiving inputs regarding the business information to be used by the other layers and components. Next, the **Risk Management Layer (RML)** focuses on the steps required to understand and analyze threats and risks. For that, the RML obtains data from monitors and inputs from the business (*e.g.*, from C-level to external advisors) to perform different tasks required to understand better and quantify the risks. Finally, the **Decision Layer (DL)** focuses on the overall cost management and selection of adequate protection. Furthermore, a **Supplementary Layer (SL)** allows for the implementation of external solutions that can support specific tasks performed by each layer or provide additional features, *e.g.*, when cyber insurance models can be considered after analyzing risks and marketplace for protections can be used to find protections. The communication between the BL, RML, and DL layers happens via the Business Manager, Risk Manager, and Decision Manager. For the SL, integration APIs are exposed to establish communication, in a standardized way (*e.g.*, based on RESTful APIs and JSON syntax), between external solutions and the framework components. Databases are not explicitly highlighted in the framework due to decisions regarding the visual representation of the framework. However, the Business, Risk, and Decision Manager components might implement their databases, whenever needed, to store and retrieve data/information.

C. Designed and Implemented Solutions

Five different solutions were designed and developed as part of the *CyberTEA* approach to perform different tasks mapped in the methodology and implement the components determined in the framework. These solutions were designed to abstract technical details as much as possible to support both technical and non-technical users during cybersecurity tasks and decision-making. The novelty of these solutions, when compared to the ones currently being used by industry, relies on the fact that it proposes and implements novel and state-of-the-art techniques to be available for companies with limitations in terms of budget and technical experts. Therefore, it addresses, especially, SMEs' demands that are not covered by expensive and complex tools available on the market. All solutions' source-code and installation guidelines are publicly available at [11].

SecRiskAI solution [9] was proposed as a Machine Learning (ML)-based approach for risk assessment of companies based on selected (and well-known) attributes, such as the number of employees, sector, and business processes. *SecBot* [3] provided a conversational agent to guide SMEs during risk management tasks and also to help the understanding of cybersecurity demands and cyberattack symptoms.

SecGrid [6] was proposed as a platform for the analysis and visualization of cyberattack traffic, thus, helping companies to understand anomalies and potential threats. *SECAdvisor* [12] provides an automated and user-friendly way to apply cybersecurity economics metrics to determine cost-efficient investments in cybersecurity. These metrics include the Gordon-Loeb model for the calculation of optimal investment in cybersecurity and the Return on Security Investment (ROSI) for the analysis of cost-effective protections.

Finally, *MENTOR* [4] is proposed as a recommender system for protections to support the decision process of selecting the best protection that fits business demands and budget. A specialized version of MENTOR called ProtectDDoS [5] was also provided to recommend protections against DDoS attacks based on cyberattack fingerprints and economic requirements.

Furthermore, four supplementary solutions were implemented to address specific challenges, including *(a)* SaCI [2], a BC-based cyber insurance model, *(b)* SHINE, a module for financial information sharing, *(c)* Kirti, a protection marketplace, and *(d)* BRAIN [8], a reverse auction for infrastructure supply. Table I summarizes the list of solutions developed in the context of the CyberTEA, including additional extensions.

TABLE I: Overview of Solutions Implemented as part of the *CyberTEA* Approach

Solution	Description	Phase Addressed of the Methodology	Components of the Framework Implemented
SecRiskAI [9]	A ML-based tool for risk assessment in companies	Phase A and B	Business Layer and Risk Analyzer
SecBot [3]	A conversational agent for cybersecurity planning and management	Phase A and B	Business Layer and Threat Advisor
SecGrid [6]	A platform for the analysis and visualization of cyberattack traffic	Phase B	Data Processor, Threat Advisor, and Risk Analyzer
SECAdvisor [12]	A GL-based tool for optimal investment in cybersecurity	Phase D	Cost Estimator and Investment Calculator
MENTOR [4]	A recommender system for protections	Phase C and D	Recommendation Engine
ProtectDDoS [5]	An extension of MENTOR for recommendation of protection against DDoS attacks	Phase A and C	Business Layer and Recommendation Engine
SaCI [2]	A BC-based cyber insurance model	Phase B	Supplementary Layer
SHINE	An economic information sharing module for the SecGrid platform	Phase B	Supplementary Layer
Kirti	A BC-based marketplace and SLA audit system for the cybersecurity market	Phase C and E	Supplementary Layer
BRAIN [8]	A BC-based reverse auction for infrastructure providers	Phase E	Supplementary Layer

The need for approaches supporting cybersecurity planning was addressed by considering technical and economic dimensions. Technical because the methodology and solutions

proposed to consider and reduce the complexity of cybersecurity tasks by providing user-friendly interfaces, technical abstractions, and automation of specific tasks (*e.g.*, risk assessment and threat analysis). The economic perspective then comes from the focus on optimizing cybersecurity costs, thus, considering all economic impacts of cyberattacks and the benefits of cybersecurity investments to plan cost-efficient cybersecurity strategies that help achieve a proper level of protection even for companies with restrictions in budget.

IV. Evaluations

Evaluations were performed to show evidence of each of the developed solutions' feasibility. These evaluations were conducted quantitatively for performance and accuracy analysis, while qualitative analysis relying on interviews and case studies was also placed to show the applications and benefits of the solutions, the methodology, and the framework.

Measurable results from the evaluations include *(a)* an end-to-end application scenario for the methodology as a case study, *(b)* the analysis of accuracy for risk assessment using SecRiskAI, *(c)* the capacity of SecBot to understand conversations and provide proper answers based on the intents of users, *(d)* the capacity of SecGrid to process a large amount of data to provide insightful visualizations and ML-based classification of cyberattacks, *(e)* the benefits of SECAdvisor and its usability for defining optimal investments and cost-effective solutions, and *(f)* the accuracy of MENTOR to recommend protections that fits the demands previously defined by companies. Also, these solutions' extensibility and integration were proven valid with proof-of-concept implementations.

A case study inspired by real-world information was performed [10] showing the phases of the proposed methodology being covered with the support of information obtained by using the proposed solutions whenever needed. Furthermore, an analysis of the economic costs of the usage of blockchain technology to ensure decentralization and immutability of cybersecurity solutions (*e.g.*, cyber insurance and marketplace) was conducted.

For the SecRiskAI, experiments with different dataset sizes (ranging from 10,000 to 50,000 entries) and information were conducted to identify their impacts on the performance of the models [9]. The experiments show that Support Vector Machine (SVM) obtains a very high accuracy in predicting risks, based on the defined model, of a company becoming the target of cyberattacks. This was analyzed with labeled datasets synthetically generated related to companies' information. More specifically, SecRiskAI was able to predict the risks of DDoS attacks and phishing correctly based on selected attributes (*e.g.*, sector, revenue, number of employees, awareness, and security controls) of the company. The SecRiskAI's experiments and results are published and available in [9].

The SecBot was evaluated regarding its capacity to extract intents and entities from conversations. The conversational agent was trained with 958 cybersecurity-related samples (*i.e.*, examples of intents and entities), and the results show it was able to cover 15 different conversation flows with 100% accuracy for the cybersecurity-related intent and entities extraction. Also, for additional flows not mapped initially, SecBot can still understand 88.33% of the conversation context to support users. These results indicated that SecBot could map the cybersecurity-related conversations for the correct intent available, thus, also being able to extract entities. Therefore, SecBot can be used to provide cybersecurity guidance against threats and also guide during risk management tasks. Part of these experiments and results are published and available in [3].

For the SECAdvisor, an independent case study was conducted to show its feasibility. Also, an usability evaluation with real-world cybersecurity teaching and consultancy activities was conducted to show the usability of SECAdvisor and its benefits to applying cybersecurity economic concepts during the planning and investments in cybersecurity. The SECAdvisor was used by hundreds of students in different courses (*e.g.*, university courses, professional certifications, and workshops) provided in European Union. It was used mainly for education of cybersecurity economics models and discussion of key steps of cybersecurity planning. It was shown that the SECAdvisor solution intuitively supports the application of cybersecurity economics models, being a low-barrier entry for not trivial cybersecurity economics methods. A running version of the tool is publicly available at [12].

For that, it relies on GL and ROSI as well as provides an integration with the MENTOR recommender system. The results of SECAdvisor are hard to measure quantitatively since it requires an exhaustive evaluation of the GL model rather than the tool itself. All of the equations and concepts proposed by the GL model over the years are replicated with perfect accuracy in the solution proposed, also allowing for the configuration of customized security breach probability functions. This helps companies and people without know-how or expertise in cybersecurity economic models to have insights into how to perform investments in cybersecurity.

Finally, the capacity of the MENTOR engine was quantitatively evaluated using a dataset of 10,000 randomly generated protection services. The experiments and results regarding MENTOR are available at [4], [5]. Such an evaluation indicates that MENTOR can recommend adequate protection services considering the price, region, and other requirements defined by end-users. The engine was developed to be scalable both in terms of user demands and the number of protections.

In summary, a set of lessons were learned from the research and experiments conducted in this PhD thesis, which includes:

- **Lesson 1.** ML-based solutions are an ally for specific cybersecurity planning tasks, but the definition of datasets with real-world data is still a challenge;
- **Lesson 2.** Solutions to process and analyze cyberattacks traffic are possible, and efficient resources usage is key;
- **Lesson 3.** Visualizations have a key role in analyzing and understanding cyberattacks behaviors;
- **Lesson 4.** Cybersecurity economic models support cost management when planning a cybersecurity strategy;

however, these models have to be calibrated according to the company's characteristics;

- **Lesson 5.** Recommendation mechanisms can be placed to filter protections and indicate adequate solutions according to companies' demands;
- **Lesson 6.** Reputation mechanisms can be an ally for the selection of protections and market analysis;
- **Lesson 7.** Blockchains are a viable approach (but with additional costs) that can be explored to simplify cybersecurity-related tasks and to develop trustworthy solutions;
- **Lesson 8.** Approaches that guide cybersecurity planning and investment are useful to support the decision-making and the adoption of cybersecurity;
- **Lesson 9.** Scientific advances and knowledge gain proved that novel models and approaches considering cybersecurity economics, cost management, and cybersecurity planning are possible and needed.

The generated results of this work and the lessons learned paved the path for the research and development of detailed cybersecurity planning and investment solutions. It impacts the field by highlighting the opportunities and benefits of multidisciplinary approaches to cybersecurity management. Thus, this work has a *(a)* a practical impact on SMEs that needs guidelines and tools to understand and conduct cybersecurity planning with an economic bias and *(b)* an academic impact on research on socio-economic models for cybersecurity and novel solutions for broad adoption of cost-efficient cybersecurity strategies.

V. Summary, Conclusions and Future Research

The contributions of this work can be summarized as the methodology, framework, and set of solutions proposed. These contributions answer all of the five RQs defined. Additional contributions include the analysis of the threat landscape and challenges that companies are facing, the investigation of cybersecurity economics to propose novel approaches that integrate the ones already existent, and the exploration of trend technologies and approaches (*e.g.*, ML, blockchain, and visualizations) to address open challenges and explore the cybersecurity planning from different perspectives.

All evaluations conducted and contributions show evidence of scientific advances in cybersecurity planning while highlighting and paving the path for stakeholders (*e.g.*, decision-makers, developers, researchers, and companies) to implement more cost-effective solutions and strategies related to cybersecurity. This also contributes to understanding the relationship and dimensions of economic and technical aspects of cybersecurity, thus, providing directions for further advances in the field and its multidisciplinary facets.

Future research includes evolving current cybersecurity economic models to fit companies' reality and showing evidence of actual benefits in real-world scenarios. Also, the measurement of the economic impacts of cyberattacks in a precise way is still a challenge. Collaboration approaches and information-sharing incentives have to be explored to address this challenge. Finally, ML-based approaches are still needed for practical measurements when not all information is known and to automate the tasks required for risk assessment.

VI. Thesis Remarks

The complete PhD thesis can be accessed at [7] or found at https://zora.uzh.ch. Further, the work conducted within this PhD was published in [3]–[12], while the source-codes of all solutions are available at [11]. This paper was supported partially by *(a)* the University of Zürich UZH, Switzerland, and *(b)* the European Union's Horizon 2020 Research and Innovation Program under Grant Agreement No. 830927, the CONCORDIA project.

References

[1] European Union Agency for Cybersecurity (ENISA), "Cybersecurity for SMEs: Challenges and Recommendations," June 2021, https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes.

[2] M. Franco, N. Berni, E. J. Scheid, B. Rodrigues, C. Killer, and B. Stiller, "SaCI: a Blockchain-based Cyber Insurance Approach for the Deployment and Management of a Contract Coverage," in *Lecture Notes in Computer Science (LNCS)*, no. 13072. Virtually: Springer, September 2021, pp. 79–92.

[3] M. Franco, B. Rodrigues, E. J. Scheid, A. Jacobs, C. Killer, L. Z. Granville, and B. Stiller, "SecBot: a Business-Driven Conversational Agent for Cybersecurity Planning and Management," in *International Conference on Network and Service Management (CNSM 2020)*, Izmir, Turkey, November 2020, pp. 1–7.

[4] M. Franco, B. Rodrigues, and B. Stiller, "MENTOR: The Design and Evaluation of a Protection Services Recommender System," in *15th International Conference on Network and Service Management (CNSM 2019)*. Halifax, Canada: IEEE, October 2019, pp. 1–7.

[5] M. Franco, E. Sula, B. Rodrigues, E. Scheid, and B. Stiller, "ProtectDDoS: A Platform for Trustworthy Offering and Recommendation of Protections," in *Economics of Grids, Clouds, Systems, and Services*. Izola, Slovenia: Springer, September 2020.

[6] M. Franco, J. von der Assen, L. Boillat, C. Killer, B. Rodrigues, E. J. Scheid, L. Granville, and B. Stiller, "SecGrid: A Visual System for the Analysis and ML-Based Classification of Cyberattack Traffic," in *IEEE 46th Conference on Local Computer Networks (LCN 2021)*, Edmonton, Canada, October 2021, pp. 1–8.

[7] M. F. Franco, "CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment," February 2023, PhD Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland, Available at https://figueredofranco.com/static/files/PhD-M-Franco.pdf.

[8] M. F. Franco, E. Scheid, L. Granville, and B. Stiller, "BRAIN: Blockchain-based Reverse Auction for Infrastructure Supply in Virtual Network Functions-as-a-Service," in *IFIP Networking (Networking 2019)*. Warsaw, Poland: IEEE, May 2019, pp. 1–9.

[9] M. F. Franco, E. Sula, A. Huertas, E. J. Scheid, , L. Z. Granville, and B. Stiller, "SecRiskAI: a Machine Learning-Based Approach for Cybersecurity Risk Prediction in Businesses," in *24th IEEE International Conference on Business Informatics (CBI 2022)*. Amsterdan, Netherlands: IEEE, June 2022, pp. 1–10.

[10] M. F. Franco, F. M. Lacerda, and B. Stiller, "A Framework for the Planning and Management of Cybersecurity Projects in Small and Medium-sized Enterprises," *Journal of Business and Projects (Revista de Gestão e Projetos)*, vol. 13, no. 3, pp. 1–25, nov 2022.

[11] M. F. Franco, "CyberTEA - Code Repository," November 2022, Available at https://gitlab.ifi.uzh.ch/users/franco/projects.

[12] M. F. Franco, C. Omlin, O. Kamer, E. J. Scheid, B. Stiller, "SECAdvisor: A Tool for Cybersecurity Planning using Economic Models," February 2023, Available at https://secadvisor.figueredofranco.com.

[13] M. F. Franco, F. M. Lacerda, B. Stiller, "SECProject: a Framework for the Management of Cybersecurity Projects in Small and Medium-sized Enterprises," in *X International Symposium on Management, Project, Innovation and Sustainability (X SINGEP)*, São Paulo, Brazil, October 2022, pp. 1–16.