

SECAAdvisor: A Tool for Cybersecurity Planning using Economic Models

Muriel Figueredo Franco^{1,2}, Christian Omlin², Oliver Kamer², Eder John Scheid^{1,2},
Lisandro Zambenedetti Granville², Burkhard Stiller¹

¹Institute of Informatics - Federal University of Rio Grande do Sul (UFRGS)

²Communication Systems Group CSG, University of Zürich UZH

E-mail: {mffranco, ejscheid, lzgranville}@inf.ufrgs.br, stiller@ifi.uzh.ch,
{christian.omlin, oliverluca.kamer}@uzh.ch

Abstract. *Cybersecurity planning is challenging for digitized companies that want adequate protection without overspending money. Currently, the lack of investments and perverse economic incentives may increase the number of cyberattacks, which result in several economic impacts on companies worldwide. Therefore, cybersecurity planning has to consider technical and economic dimensions to help companies achieve a better cybersecurity strategy. This paper introduces SECAAdvisor, a tool to support cybersecurity planning using economic models. SECAAdvisor allows one to (a) understand the risks and valuation of different businesses' information, (b) calculate the optimal investment in cybersecurity for a company, (c) receive a recommendation of protections based on the budget available and demands, and (d) compare protection solutions in terms of cost-efficiency. Furthermore, evaluations on usability and real-world training activities performed using SECAAdvisor show its efficacy and usability, allowing users to explore economic concepts and models for cybersecurity planning.*

1. Introduction

One challenge for cybersecurity is how to plan a cybersecurity strategy without overspending money on protection measures [Franco et al. 2023]. The cybersecurity market is worth billions of dollars and steadily rising investments, with companies investing in cybersecurity to ensure availability and protect their core businesses from economic losses. These losses might include direct losses due to business interruption (e.g., an e-commerce that cannot offer products due to server downtime) or indirect losses like reputation harm and legal penalties.

Although there are businesses more prone to specific attacks, in general, attackers tend not to spend too much time focusing on one specific company but on exploring vulnerabilities in the type of businesses they see as potential weaknesses. This happens especially in the case of Small and Medium-sized Enterprises (SMEs), which are the focus of more general attacks (i.e., not tailored for a specific company) [European Union Agency for Cybersecurity (ENISA) 2021] because attackers know the reality of most SMEs: lack of training, limited technical expertise, and insufficient budget for cybersecurity.

Cyberattacks can devastate SMEs and put many companies out of the market in the last few years. Therefore, it is important to understand and mitigate risks to reduce possible impacts on their operations [Franco et al. 2021]. However, most companies do not have sufficient budgets to spend, making cybersecurity planning harder. Therefore, it is important to have tools and models that simplify the task of cybersecurity planning, making it not only more user-friendly but also more cost-efficient. Thus, approaches

that rely on cybersecurity economics concepts have to be considered [European Union Agency for Cybersecurity (ENISA) 2012a] together with technical knowledge to balance risks and investments for a company.

In cybersecurity economics, the Gordon-Loeb (GL) model is the most well-accepted analytical model to determine the optimal investment level in cybersecurity [Gordon and Loeb 2002a]. The model considers (a) how much the data or service is valued, (b) how much the data is at risk (e.g., attack probability-based historical data), and (c) the probability that an attack is going to be successful, which can be defined based on the threat modeling and risk analysis. Also, extensions to the GL model have been proposed over the years.

In the last years, information segmentation was also introduced as a key element for investments in cybersecurity [L. A. Gordon, M. P. Loeb, L. Zhou 2021]. The information segmentation argues that the amount invested in cybersecurity, when calculated using the GL model, should be considered in terms of specific information segment and their potential benefits (i.e., investments vs. potential losses). However, this kind of model is not trivial to be applied by companies, nor is it well-known by non-technical users. Therefore, solutions that support the application of GL and other economic metrics to cybersecurity are welcome for companies' faster adoption since economic motivation is one of the strongest to convince a company to invest in cybersecurity.

Based on that, SECAdvisor, an open-source and visual tool for calculating the optimal investment in cybersecurity, is proposed. SECAdvisor is the first of its kind. It allows users to define information segments within a company and calculate the optimal investment for each segment, including potential losses with and without an optimal investment in cybersecurity. This calculation applies GL to estimate values accurately. After calculating optimal investments in cybersecurity, SECAdvisor can recommend protection measures using an external recommendation engine [Franco et al. 2019]. Furthermore, the Return On Security Investment (ROSI) metric is calculated for each recommended solution to compare the cost-effectiveness of protections.

The remainder of this paper is organized as follows. Section II introduces key economic models, while Section III reviews related work on cybersecurity economic solutions. Section IV presents the SECAdvisor tool, followed by evaluations as of Section V. Finally, Section V concludes the article.

2. Background

This section introduces the theoretical foundations of two of the most well-accepted cybersecurity economics models, including examples for cost analysis and investments in cybersecurity. These models are used as the basis for conducting cybersecurity planning under an economic lens using the SECAdvisor tool.

2.1. Gordon-Loeb (GL) Model

The GL model is an economic model used to analyze the optimal investment level in cybersecurity. The model was proposed in 2002 by Gordon and Loeb [Gordon and Loeb 2002b] and considers a system's vulnerability and potential financial loss due to a cyber-attack. There are two generic security breach classes (i.e., definitions for $S(z, v)$) to show the performance of the GL model to estimate the optimal investment in cybersecurity. The purpose of a cybersecurity investment is to lower the probability that a system within the company will have a financial loss. Thus, the GL model was initially demonstrated

using these two security breach probability functions. The first class refers to a linear vulnerability, while the second analyzed class is concave (*i.e.*, the slope of the graph line increases gradually from left to right). It is important to note that, based on the analysis conducted, the optimal investment in cybersecurity is always $\leq \frac{1}{e}$, where e is the Euler's constant (*i.e.*, ≈ 2.71828). This means that the optimal investment is always $\leq 37\%$ of the expected loss (vL) without investments [Baryshnikov 2007].

Therefore, GL determines, in a general way, that the maximum investment (z_{max}) in cybersecurity will never exceed 37% of the expected loss (vL) for all functions part of the classes investigated by [Gordon and Loeb 2002b]. To calculate the optimal investment, it is necessary to use the productivity of a cybersecurity investment, which may vary for different scenarios, depending on specific concerns surrounding a particular set.

The optimal amount (z_i^*) to invest in a specific information segment i depends on the value of the information (L_i) that is part of the segment. Also, the vulnerability of each segment (v_i) has to be considered for calculating the productivity of additional investments in cybersecurity for each segment. Therefore, the total cost of investment results in the sum of each segment calculated individually. Hence, it is possible to prioritize segments based on cost-benefits and achieve a better overall cybersecurity investment. The Equation 1 shows how to calculate the new vulnerability v for a given investment z . This means that, for this scenario, the optimal investment must find the better trade-off between v and z .

$$S(z, v) = \frac{v}{1 + \frac{1}{L \times \alpha} \times z}, \text{ where } \alpha = 0.001 \text{ (Productivity Coefficient), } v = \text{Vulnerability,}$$

$$L = \text{Potential Loss, } z = \text{Investment} \quad (1)$$

2.2. Return On Security Investment (ROSI)

The concept of ROSI is slightly similar to the Return on Investment (ROI). However, while ROI measures the benefits/profits from a particular investment, ROSI focuses on the loss prevented by a cybersecurity investment. ROSI is a cybersecurity economics metric that helps to identify when a given solution (*e.g.*, Firewall, Antivirus, or Cybersecurity-as-a-Service product) is cost-efficient or not [Sonnenreich et al. 2005, European Union Agency for Cybersecurity (ENISA) 2012b]. Also, this metric is beneficial when comparing two different solutions with similar characteristics to determine which one should be acquired from an economic perspective.

A desirable result is a $ROSI \geq 1$, which means the payback is positive. If $ROSI$ is ≤ 1 , there is no cost-benefit in investing in the specific solution. Therefore, the higher the $ROSI$, the better the investment in a solution. $ROSI$ general calculation is provided in Equation 2. As can be seen, for the calculation of $ROSI$, it is necessary to quantify the monetary risk of a cyberattack. Therefore, analytical approaches must be in place to help companies determine the possible financial losses due to a cyberattack.

$$ROSI = \frac{Risk_{Reduction} - Solution_{Cost}}{Solution_{Cost}}, \text{ where} \quad (2)$$

$$Risk_{Reduction} = ALE \times Mitigation_{Ratio}$$

Besides the solution's cost and efficiency (*i.e.*, mitigation rate), ROSI uses the Annual Loss Expectancy (ALE) as input. The calculation of ALE is shown in Equation 3. For that, it is necessary to estimate the Annual Rate of Occurrence (ARO) of cybersecurity incidents and also the Single Loss Exposure (SLE), which means that an analysis of the company has to be made to understand the history of the attacks to identify its behaviors and impacts in the company. SLE can be described as the cost of a loss due to a single incident, while the ARO is the probability of an incident happening within a year timeframe.

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

ALE: Annual Loss Expectancy
ARO: Annual Rate of Occurrence
SLE: Single Loss Exposure

(3)

3. Related Work

The solutions surveyed for this work are tools, systems, or software that implement methodologies or techniques to allow users to handle cybersecurity demands more intuitively. These solutions discussed in this section provide at least (*a*) a backend that implements a set of features for cybersecurity planning and investment and (*b*) a frontend that allows users to interact with the solution to access the features. Therefore, solutions like those discussed below are essential for cybersecurity planning and investment, especially for SMEs needing intuitive and simplified ways to handle cybersecurity. An overview and comparison of different solutions discussed within this section is shown in Table 1.

The Cybersecurity Osservatorio offers services to raise SMEs' cybersecurity awareness, including a self-assessment tool for cyber risk. This tool requires inputs about security measures and key assets to estimate expected annual losses for relevant threats, providing results when all information is correctly submitted. Similarly, a recommender system proposed by [Huff et al. 2021] tracks and recommends protections against vulnerabilities using Natural Language Processing (NLP), fuzzy matching, and Machine Learning (ML). Tested on 50 software and hardware inventories, it saved over 7 hours of work and provided more accurate results than human analysts. This system is noted as the first automated solution for matching vulnerabilities in private software and hardware inventories.

A recommender system for data protection was introduced by [Li et al. 2019], which simulates protection options and provides insights into aggregated plans. The system recommends protections for a given data group to achieve a higher risk deduction with a given budget. Even though this work can be the first step toward data-centric security application, the authors emphasize that evaluations with larger samples are still needed to validate and improve the proposed system. Similarly, MENTOR [Franco et al. 2019] was also proposed as a recommender system for protections relying on correlation measurements to determine which protections fit better businesses' demands (*e.g.*, type of attack, region, and leasing period) and budget available. MENTOR was integrated with different solutions in the cybersecurity planning process, such as the conversational agent for cybersecurity planning proposed in [Franco et al. 2020a] and the blockchain-based marketplace for protections introduced in [Franco et al. 2020b].

Table 1. Comparison of Solutions for Cybersecurity Planning and/or Investment

Solution	Category	Type	User-Friendly Interface	Technical Aspects	Economic Aspects	Characteristics
[Cybersecurity Osservatorio]	Risk Assessment	Product	Yes	Partially	Yes	Provides report on expected annual losses.
[Rea-Guaman et al. 2018]	Risk Assessment	Research and Prototype	Yes	Partially	Partially	Correlation between Vulnerabilities and Assets.
[Huff et al. 2021]	Recommender System and Risk Assessment	Research and Prototype	No	Yes	No	NLP and ML techniques are applied to list vulnerabilities in a software inventory.
[Hallman et al. 2020]	Cybersecurity Investment	Research and Prototype	Yes	Partially	Yes	Quantifies the effects of cybersecurity investment in critical infrastructures.
[Benz and Chatterjee 2020]	Risk Management	Research and Prototype	No	Yes	Partially	Questionnaire-based tool with 35 questions based on NIST CSF.
[Huang et al. 2019]	Risk Management	Research and Prototype	Yes	Yes	No	Visual tool that simplifies and automates the application of NIST CSF in companies.
[Li et al. 2019]	Recommender System and Cybersecurity Planning	Research and Prototype	Yes	Yes	Yes	Provides recommendation for data protections based on risk factors and a given budget.
[Franco et al. 2019]	Recommender System for Protections	Research and Prototype	Yes	Partially	Partially	Provides recommendation for protections based on technical demands and a given budget.

In another work based on the NIST Cybersecurity Framework (CSF), the authors proposed a user-interactive cybersecurity tool to simplify and automate the NIST compliance of companies [Huang et al. 2019]. This work developed a front-end and back-end to provide a robust and user-friendly NIST-compliance guideline tool. However, even simplifying the process by providing Web-based interfaces and other features, applying the NIST CSF remains a challenge for SMEs since it requires an understanding of cybersecurity-related information, concepts, and interactions.

In [Rea-Guaman et al. 2018], a new solution for the analysis and risk management was proposed. The novelty of the solution relies on the correlation between vulnerabilities and the assets available in the company. Understanding the potential impacts on the assets is possible if a given vulnerability is exploited or an incident happens. The authors argued that there is a gap in the literature that concerns technical and economic impacts since most of the solutions available for risk management focus on threats without understanding the assets and their possible economic impacts.

A tool named ReCIs was introduced in [Hallman et al. 2020]. The tool applies the Return on Cybersecurity Investment (ROCI) model, also proposed by the authors of the work, to quantify the effect of cybersecurity investment on critical infrastructure. In the ROCI model, the ultimate return value to determine if protection is cost-efficient is calculated as the annual difference between costs associated with cyberattacks minus the costs of those same attacks, now mitigated by a cybersecurity solution. This work was one of the first cybersecurity investment approaches to quantify a return on investment for

the critical infrastructure sector. Also, there are industry efforts for economic analysis by relying on cyber risk quantification models, such as the QBER model [Franco et al. 2024] proposed as an attempt to standardize the economic analysis within the Indian financial sector.

Based on the literature review, cybersecurity is receiving much attention on different fronts, from mitigating cyberattacks to planning and investing in defining cybersecurity strategies. Most cybersecurity economics models are still not mature [Kianpour et al. 2021] but are evolving into more robust models. Therefore, it is important to provide tools that help companies understand and apply current and future economic models in straightforward ways. Thus, there are opportunities for multidisciplinary approaches to address cybersecurity gaps, focusing on more efficient, economically viable, and suitable cybersecurity strategies.

4. The SECAdvisor Tool

The SECAdvisor is a solution proposed to support the definition of budget, requirements, and information during the cybersecurity planning of companies. To the best of the authors' knowledge, SECAdvisor is the first solution to integrate different cybersecurity economic models in cybersecurity planning in a straightforward and extensible way. The solution was designed and developed to support companies but also to support training and educational activities with people interested in cybersecurity planning, such as consultants, academic students, and researchers.

Figure 1 gives an overview of the conceptual architecture of SECAdvisor, including three different application layers and their relationships. The flow starts with the decision-maker (*i.e.*, user) accessing the Web-based Interface of SECAdvisor and defining the business profile representing the company they want to conduct the calculations. To create such a profile, the user must submit key information about the company to SECAdvisor, such as the revenue, sector, and number of employees. Next, the Segment Layer is in charge of (*a*) managing the different segments within the company, (*b*) estimating how valuable each segment is (*e.g.*, based on the critical data available and specific parameters for a given segment), (*c*) calculating and comparing the optimal investment per segment, and (*d*) configuring the Breach Probability Function (BPF) according to the needs. Finally, the *Recommendation Layer* allows for the selection of specific threats and, based on the optimal calculation provided by the *Segment Layer*, can determine which protections are suitable for the company in terms of fitting the optimal investment, budget available, and demands to mitigate/avoid a selected threat.

The *Recommendation Layer* prepares all information required and makes requests to the recommendation engine implemented by MENTOR [Franco et al. 2019], which uses Euclidean Distance, Pearson Correlation, and Manhattan Distance as similarity algorithms. After a list of protections is recommended for the company, the SECAdvisor calculates the ROSI metric for each protection since it can support cost-efficient investments by comparing different recommended protections. The *Data Layer* is also implemented by SECAdvisor to store all relevant data (*e.g.*, information regarding the business, segments, and knowledge used for the segments estimations). Besides that, all configurations needed for the GL model and for the customization of the SECAdvisor are stored in a database. Therefore, although predefined equations and configurations are placed, the SECAdvisor can be extended and adapted by changing key fields in the database.

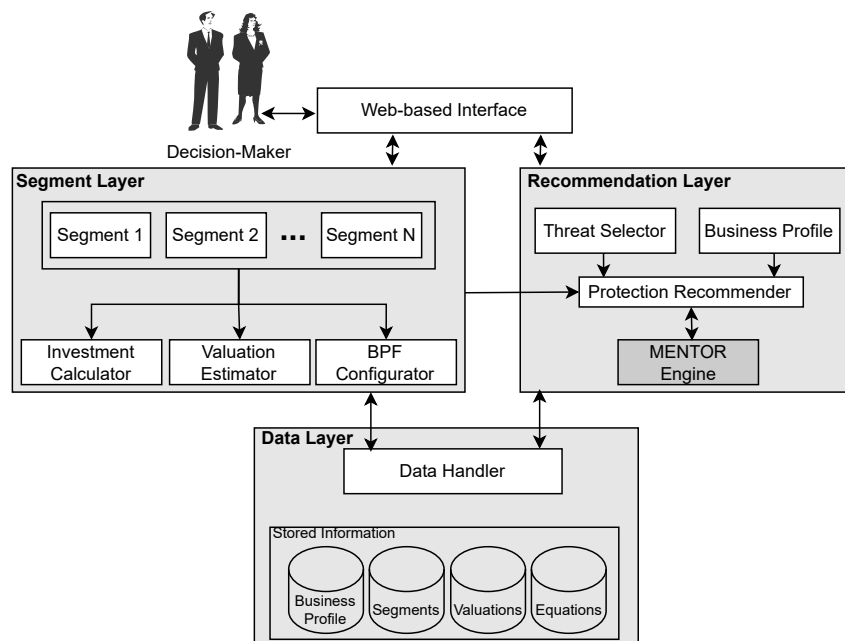


Figure 1. Conceptual Architecture of the SECAdvisor

4.1. Segments and Value Estimation

Determination of the segments and their values is critical for the optimal calculation of investments and the recommendation of protections according to specific demands [L. A. Gordon, M. P. Loeb, L. Zhou 2021]. A segment represents a technical business area of a company. Thus, the optimal investment amount should be calculated per segment, since a specific segment might be directly related to the potential benefits of cybersecurity investments. The following information is required to determine a new segment:

- **Segment Name:** The parameter represents the segment's name, which can be freely chosen by the company (*i.e.*, user).
- **Segment Type:** The type of segment is used to suggest suitable cybersecurity threats and simplify the segment's monetary valuation. SECAdvisor allows for the selection of different pre-defined segments, such as *Web Server*, *Network*, or *Database* segments.
- **Value:** To calculate the optimal cybersecurity investment level, the segment's monetary value (US\$) is needed. Since it is often difficult to determine this value, the SECAdvisor assists in valuing the segment based on publicly available reports and data. For example, for database segments, it can take statistics from data leakage reports [Corporation 2022] and compute expected loss in case of leakage based on the number and type of records available.
- **Risk:** The *Risk* parameter describes the probability of a cyberattack. The user is allowed to specify a number between 0% and 100%. This parameter is needed to determine the optimal investment. The accuracy of such information will vary according to the user's knowledge and risk assessments previously conducted.
- **Vulnerability:** This parameter is also needed to calculate the optimal cybersecurity investment. It describes the probability that a cybersecurity attack on the segment will be successful. Values between 0% and 100% are allowed, which will vary according to the user's knowledge of the risk.

Next, the value of the segment must be estimated. However, it is not a trivial task for a user to determine the monetary value of the segment, such as how much a database is worthy for the business or networking infrastructure based on, for example, the records available in the database and its value in case of leakage. Therefore, the SECAdvisor provides aid to facilitate this decision. The system allows the user to enter parameters tailored to the segment, which are evaluated based on previous knowledge populated in the database (*e.g.*, values based on estimations made by reports, research, or shared by partners). Thus, the user can receive a suggestion for the segment's value, which he/she can use or adapt according to his/her view.

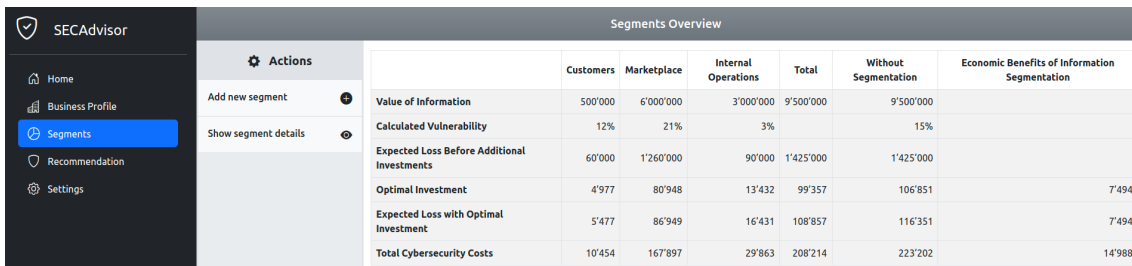
4.2. Investment Calculation

The SECAdvisor calculates the optimal cybersecurity investment based on an extension of the GL model proposed by [L. A. Gordon, M. P. Loeb, L. Zhou 2021]. This extension combines the GL with the idea of information segmentation. An important factor for the investment calculation is the BPF. It is denoted as $S(z, \nu)$, where z describes the monetary investment and ν the vulnerability of the segment. The BPF describes the productivity of the investment, which first increases and then decreases after a certain point. Each additional investment is higher than the resulting benefit from this point on. The steps and definitions described in Section II are used to showcase the application of the GL model within SECAdvisor.

To calculate the optimal investment in cybersecurity, the SECAdvisor uses the BPF defined in Equation 4. This BPF is an extension provided by the GL model considering different segments of information within a company. It provides a slightly different behavior when compared to the one initially provided by the GL model (*cf.* Equation 1), thus showing how the BPF can be adapted for different scenarios. Thanks to this GL model extension, the SECAdvisor calculates the optimal investment level for each segment. In addition, the monetary advantage of information segmentation is also illustrated in the application. Note that these equations are fully extracted from the original work that extended the GL model to support information segmentation [L. A. Gordon, M. P. Loeb, L. Zhou 2021]. Therefore, it tries to generalize the BPFs to cover hypothetical scenarios anchored by some assumptions related to the reality of cybersecurity today. However, this is not true for any company that wants to invest in cybersecurity since different companies' sizes, sectors, and security landscapes may require adjustments on the BPF to accurately calculate. Thus, for an accurate optimal investment calculation, the BPF has to be defined according to the reality and demands of a given company or sector.

$$S_i(z_i, \nu_i) = \frac{\nu_i}{1 + \frac{1}{L \times 0.001} \frac{z}{L_i}} \quad (4)$$

To determine the cost-effectiveness of a cybersecurity investment, the SECAdvisor then uses the ROSI metric. This metric is used because cybersecurity investments do not bring a direct profit but reduce potential damage. During the evaluation of cybersecurity investments, the focus is on assessing how much potential loss can be prevented by an investment. Therefore, the monetary value of the investment must be compared with the monetary value of the risk reduction.



	Customers	Marketplace	Internal Operations	Total	Without Segmentation	Economic Benefits of Information Segmentation
Value of Information	500'000	6'000'000	3'000'000	9'500'000	9'500'000	
Calculated Vulnerability	12%	21%	3%		15%	
Expected Loss Before Additional Investments	60'000	1'260'000	90'000	1'425'000	1'425'000	
Optimal Investment	4'977	80'948	13'432	99'357	106'851	7'494
Expected Loss with Optimal Investment	5'477	86'949	16'431	108'857	116'351	7'494
Total Cybersecurity Costs	10'454	167'897	29'863	208'214	223'202	14'988

Figure 2. Dashboard of SECAdvisor with the Optimal Investments per Segment Calculated

4.3. SECAdvisor's Implementation

The SECAdvisor was mainly implemented using *AngularJS* and *NestJS* frameworks. The database is the *MongoDB*, a document-oriented NoSQL database management system. The data used for the SECAdvisor prototype is stored on *MongoDB Atlas*, a flexible and scalable cloud database service. The database was connected using the *Mongoose*, an Object Data Modeling (ODM) library for Node.js. Calculating the optimal investment level is a core competence of the application. For that, the library *nerdamer* was used to enable calculation operations that JavaScript does not provide by default. Finally, the integration with the recommender system, the so-called MENTOR, was performed by making calls for a RESTful API implemented by MENTOR. The source code and a full-fledged prototype of SECAdvisor are publicly available ¹.

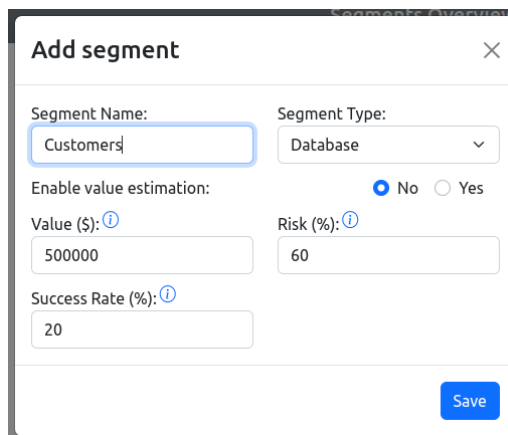


Figure 3. Definition of Segments Using the SECAdvisor Interface

For the tool's usage, as the first step after the login, the user has to add his/her business profile and the segments that compose the business under analysis. The user can use the SECAdvisor interface to add each segment required for the optimal investment calculation. Figure 3 shows the interface for adding one segment. A database segment (*i.e.*, segment type) is selected, which requires the user to fulfill the information regarding the records stored in such a database (*e.g.*, number of records with sensitive and anonymized data). If this information is available, the value estimation can be performed automatically; otherwise, the segment's value must be defined manually. Also, the risk of an attack happening in this segment has to be defined together with the likelihood of a successful attack.

¹<https://gitlab.ifl.uzh.ch/franco/secadvisor/>

After having the segments determined (*i.e.*, value, risk, and vulnerability of a segment), optimal investments can be calculated by applying the GL model automatically. The equations are used as defined by the database (*e.g.*, BPF and additional calculations). Figure 4 shows the calculations made for each segment added to the SECAdvisor. In this example, three segments are available: Customers Database, Marketplace server, and Internal Operations network. An overview of information is available in the table generated by SECAdvisor, and the optimal investment is defined.

Furthermore, to explain the calculations in detail, SECAdvisor provides a feature that shows the different values computed until finding the optimal investment, including values higher and lower than the final value. Figure 5 depicts the ENBIS rate for each value calculated until finding the optimal investment (highlighted in the green row). Also, the user can customize his/her investment to check if there is a positive ENBIS. Such a feature helps to understand if the current investment decisions are efficient compared to the optimal investment.

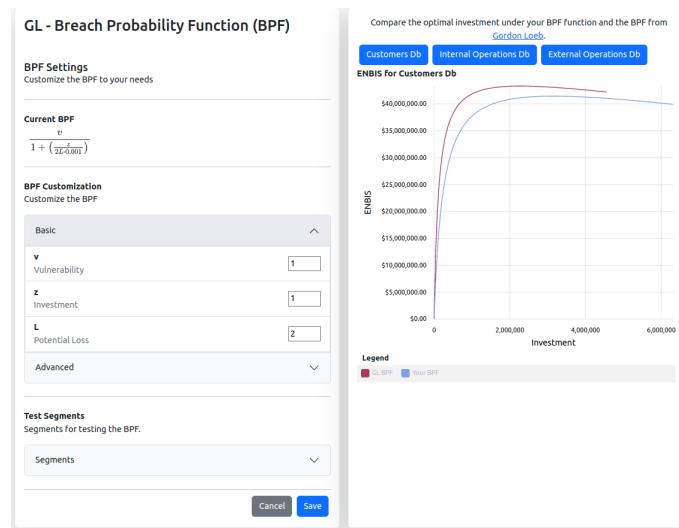


Figure 4. Interface for Customization of BPF using SECAdvisor

The BPF can also be configured according to the preference of the company. Figure 4 shows this configuration feature. SECAdvisor uses, as default, the BPF introduced in [L. A. Gordon, M. P. Loeb, L. Zhou 2021] but allows for (a) changing the weight of each variable part of the equation (*i.e.*, basic configuration) or (b) defining a complete new BPF (*i.e.*, advanced configuration). Moreover, it is possible to compare different BPFs with the original one provided by the GL model. Thus, users can adjust the BPF according to their companies' reality to calculate the optimal investment.

After the optimal investment calculation, the user can use this information as input for the next steps of planning and investment, taking it as a reference value for each segment. For instance, this value can determine the maximum budget to spend with protections for a specific segment. With this amount at hand, the user can then go for the *Recommendation tab*, which allows obtaining recommendations of protections based on the MENTOR engine. Besides recommending protections that fit the budget (*i.e.*, optimal investment) and customized demands, the SECAdvisor calculates the ROSI metric by just clicking right below one suggested protection.

Investment Analysis - Marketplace

Investment	Breach Probability	EBIS	ENBIS Rate
25000	0.041	1'016'129.032	991'129.032
0	0.21	0	0
10'000	0.079	787'500	777'500
20'000	0.048	969'230.769	949'230.769
30'000	0.035	1'050'000	1'020'000
40'000	0.027	1'095'652.174	1'055'652.174
50'000	0.023	1'125'000	1'075'000
60'000	0.019	1'145'454.545	1'085'454.545
70'000	0.017	1'160'526.316	1'090'526.316
80'000	0.015	1'172'093.023	1'092'093.023
80'948	0.014	1'173'051.479	1'092'103.479
90'000	0.013	1'181'250	1'091'250
100'000	0.012	1'188'679.245	1'088'679.245
110'000	0.011	1'194'827.586	1'084'827.586
120'000	0.01	1'200'000	1'080'000
130'000	0.009	1'204'411.765	1'074'411.765
140'000	0.009	1'208'219.178	1'068'219.178
150'000	0.008	1'211'538.462	1'061'538.462
160'000	0.008	1'214'457.831	1'054'457.831

Figure 5. Interface for Customization and Zoom-In on the Optimal Investment Calculation

The ROSI calculation can be done for each protection recommend, which requires the user to provide the mitigation rate, the incident cost, and the annual incidence rate for each protection, as shown in Figure 6. According to the segment definition, these values have already been received from the MENTOR recommendation engine and provided by SECAdvisor. However, the user can manually edit this if needed.

Calculate ROSI

Mitigation Rate(%): 60

Cost of Incident(\$): 4000000

Annual Rate of Incidence: 2

Cancel Calculate ROSI

Figure 6. Input Parameters for ROSI Calculation using SECAdvisor

5. Evaluations

The evaluation conducted on SECAdvisor focuses on (a) the usability and benefits of SECAdvisor, as well as (b) highlights examples of successful practical activities conducted using SECAdvisor for educational purposes in European cybersecurity courses.

It is important to note that the evaluation of the GL model is explicitly out of the scope since it is already extensively evaluated in the literature, such as in [Baryshnikov

2007, H. R.K. Skeoch 2021, L. A. Gordon, M. P. Loeb, L. Zhou 2021]. Therefore, this section focuses on evaluating the capacity of the SECAdvisor tool to achieve the correct values of optimal investments by applying the GL model and its usability to reduce the barrier to applying cybersecurity economic models. Also, the recommendation process was evaluated in previous research available at [Franco et al. 2019].

5.1. Usability

For the usability evaluation, a survey was conducted on the platform’s usability and intuitiveness for cybersecurity investment calculations. Real-world users were invited to use the platform to fulfill a given set of tasks and rate its usability on a System Usability Scale (SUS) questionnaire [Brooke 1996].

Thirteen people participated in the evaluation of the SECAdvisor. All users had previous experience in computer science, but only three were cybersecurity experts. Furthermore, most of the participants knew basic concepts about business planning, but only two of them had practical business experience. All users could create an account on the platform and log in to the tool. All participants were able to use the tool successfully and did not face any technical problems. Survey participants all ranged in the age group of 20 to 49, with the majority of respondents (7) from 20 to 29.

Users were asked to create an account and configure SECAdvisor with essential information for three segments: Web Server, Database, and Network. After this initial configuration, a set of tasks was defined and conducted to evaluate different features implemented in the SECAdvisor tool. They were tailored to validate if most users can find correct results by applying cybersecurity economics principles intuitively and user-friendly. Table 2 summarizes the tasks conducted and their success rate. A task was considered successfully solved if the answer matched the correct answer. For all tasks, the majority of the participants were able to solve the task successfully and provide the correct answer.

Table 2. Tasks Performed by Participants using the SECAdvisor

Task	Question	Answer	Success Rate
1	What is the vulnerability of the Database?	8%	92%
2	What is the yearly expected loss of the Database if there are no additional investments in cybersecurity?	\$ 24,576	100%
3	After adding all the segments in the tool, how much is the economic benefits between the investment using information segmentation and without information segmentation considering the optimal investment?	\$ 1,852	77%
4	How much is the total costs of cybersecurity for all of the segments?	\$ 41,079	92%
5	Which recommendation provides the highest ROSI for the Network segment?	Portwell	92%
6	What is the optimal investment for the Database segment after adjusting for 1.5 the weight of the vulnerability (v) on the BPF?	\$ 3,058	69.2%

Task 1 had a 92% success rate, with only one incorrect response likely due to a form error. Task 2 had a 100% success rate, unsurprising given its similarity to Task 1. Task 3’s success rate was 77%, lower due to participants’ unfamiliarity with the GL

model's information segmentation concept and the task's complexity. Task 4 had high success, with one error involving the correct total cost but the wrong parameters.

For Task 5, participants had to navigate from the segment overview table to the recommendation section, with most solving it successfully except for one incorrect response, highlighting their familiarity with ROSI. This indicates that users could navigate to the recommendation page, input data, and compare ROSI values, showcasing the tool's effectiveness even for those with little prior experience. Task 6 had the lowest success rate at 69.2%, as it required adjusting the BPF, which most users were unfamiliar with. However, this lower success rate is not overly concerning since the tool provides a default function that is well-researched and widely accepted, making custom input unnecessary for regular use.

The overall success rate is high, with 87.2% of correct answers. This means that most participants in the evaluation were able to use the tool properly and use its support to solve the tasks successfully. All evaluation participants had a technical background, were expected to be above average in technical skills, and were more likely to figure out how the system works successfully. Finally, a final score was calculated according to the SUS.

All ten SUS questions are initially scored from 0 (Strongly Disagree) to 4 (Strongly Agree). Next, odd-numbered questions are positively worded, so it is subtracted 1 from the user's response score, while even-numbered questions are negatively worded, resulting in a subtraction of the user's response from 4. After the score adjustment, the sum of all answers is obtained (a value from 0 to 40). It is then multiplied by 2.5 to get a score from 0 to 100. This score is not a percentage; a score above 70 is satisfactory. The overall SUS score was 82.1, indicating that SECAdvisor has very good usability and offers essential features for user-friendly application of cybersecurity economic metrics. There were three outliers in the SUS scores. The first, with expertise in "Informatics," provided no additional feedback. The second, an expert in "Cybersecurity and Risk Management," had a high understanding, showing the tool benefits from specific domain knowledge. The third, with the lowest score, struggled to understand the system without step-by-step guidelines.

5.2. Real-World Practical Activities

A set of practical educational activities was conducted using SECAdvisor. This allowed hundreds of people and participants to get in contact with cybersecurity economics concepts for the first time or even – when the knowledge was existent – to understand scenarios where it can be applied usefully.

The SECAdvisor was already part of the course "Becoming a Cybersecurity Consultant"², which is part of a certification initiative developed within the H2020 CONCORDIA project to support people in preparing for a career as a cybersecurity consultant. SECAdvisor was used for a 90-minute practical exercise conducted with 120 participants after the theory on cybersecurity planning with an economic bias. The exercises supported by SECAdvisor included the (a) calculation of optimal investments in cybersecurity using the GL model, (b) identification of protection candidates that fit specific companies' demands, and (c) selection of cost-effective protections from a list of candidates using automated calculation of the ROSI metric. All participants could apply the concepts, and

²<https://www.concordia-h2020.eu/becoming-a-cybersecurity-consultant/>

the feedback was mainly positive, highlighting SECAdvisor as the first tool that provides many benefits for both practical application in industry and education.

Also, SECAdvisor was used for practical exercises during cybersecurity lectures for 40 Master's students at the University of Zürich. This helped them understand practical applications of cybersecurity concepts and conduct planning tasks. Finally, SECAdvisor was part of a 180-minute tutorial on the European Network for Cybersecurity (NeCS) PhD School. Around 30 participants, all at the doctoral level and with experience in cybersecurity, had the opportunity to interact with SECAdvisor to conduct five practical tasks for cybersecurity planning. Besides the exercises mentioned above, the tutorial also included the definition of customized security BPFs and a comparison of the current cybersecurity investment budget against the optimal investment.

6. Conclusions and Future Work

Solutions like SECAdvisor can benefit SMEs (and also large companies) around the globe in better planning and investment decisions in cybersecurity while supporting the analysis of possible financial losses due to a successful cyberattack. Besides cybersecurity solutions, key investments must be made to increase cybersecurity staff and promote cybersecurity awareness for their general employees. Therefore, companies must ensure they can detect and mitigate cyberattacks effectively, using a clear cybersecurity strategy tailored to the company's reality, thus, targeting personnel culture, size, sector, and budget, while covering all relevant facets of cybersecurity.

The evaluations and activities performed with several real-world users prove the benefits and feasibility of SECAdvisor for disseminating and applying cybersecurity economic concepts for different stakeholders (*e.g.*, educators, consultants, security experts, and researchers). The tasks performed during the usability evaluation provide a high task success rate when used by people with technical knowledge, and even advanced features can be employed successfully. The tool strives to fulfill different criteria by providing relevant features, such as user-friendly interaction for non-technical users and simplifying the calculation of the optimal investment in cybersecurity. Some complexities and gaps must also be considered as part of our evaluation. For example, the accuracy of the results depends on the (*a*) quality of risk assessment and data provided as input, (*b*) level of knowledge of the user to configure the system, and (*c*) the calibration of the GL model. However, based on our experience, it is clear the benefit of SECAdvisor is to introduce concepts of cybersecurity economics and highlight the flow of cybersecurity planning under the economic lens.

Future work includes evaluating the tool with the industry using data for real vulnerabilities, threats, and controls. Also, Monte Carlo simulations can improve the input details based on statistical simulations using real-world data. Furthermore, simulation can assess the tool's decisions and compare the GL model to real-world scenarios. The customization of the BPF can also be enhanced to be more intuitive and automated based on different profiles of companies and sectors. Finally, investigations on novel cybersecurity economic models can be conducted, including the applications of techniques to infer correctly the information needed for the calculation of cybersecurity investments.

Acknowledgements

This work was partially supported by (a) the University of Zürich UZH, Switzerland and (b) the São Paulo Research Foundation (FAPESP) under grant number 2020/05152-7, the PROFISSA project, and is part of CNPq process 316662/2021-6. It is also part of the INCT of Intelligent Communications Networks and the Internet of Things (ICoNIoT), funded by CNPq (proc. 405940/2022-0) and the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) Finance Code 88887.954253/2024-00.

References

- Baryshnikov, Y. (2007). IT Security Investment and Gordon-Loeb's 1/e rule. Berlin, Germany, June, https://econinfosec.org/archive/weis2012/papers/Baryshnikov_WEIS2012.pdf.
- Benz, M. and Chatterjee, D. (2020). Calculated Risk? A Cybersecurity Evaluation Tool for SMEs. *Business Horizons*, 63(4):531–540.
- Brooke, J. (1996). *SUS: A 'Quick and Dirty' Usability Scale*, chapter 21, pages 189–194. Taylor & Francis, London.
- Corporation, I. (2022). Cost of a Data Breach Report 2022. Available at <https://www.ibm.com/security/data-breach>.
- Cybersecurity Osservatorio. Self assessment questionnaire. November 2022, Available at <https://www.cybersecurityosservatorio.it/en/Services/survey.jsp>, last visit November 2022.
- European Union Agency for Cybersecurity (ENISA) (2012a). Economics of Security: Facing the Challenges. <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/EoSFinalreport>.
- European Union Agency for Cybersecurity (ENISA) (2012b). Introduction to Return on Security Investment: Helping CERTs Assessing the Cost of (Lack of) Security. <https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment>.
- European Union Agency for Cybersecurity (ENISA) (2021). Cybersecurity for SMEs: Challenges and Recommendations. Available at <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>.
- Franco, M., Rodrigues, B., Scheid, E. J., Jacobs, A., Killer, C., Granville, L. Z., and Stiller, B. (2020a). SecBot: a Business-Driven Conversational Agent for Cybersecurity Planning and Management. In *International Conference on Network and Service Management (CNSM 2020)*, pages 1–7, Izmir, Turkey.
- Franco, M., Rodrigues, B., and 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)*, pages 1–7, Halifax, Canada. IEEE.
- Franco, M., Sula, E., Rodrigues, B., Scheid, E., and Stiller, B. (2020b). ProtectDDoS: A Platform for Trustworthy Offering and Recommendation of Protections. In *Economics of Grids, Clouds, Systems, and Services*, Izola, Slovenia. Springer.
- Franco, M., von der Assen, J., Boillat, L., Killer, C., Rodrigues, B., Scheid, E. J., Granville, L., and Stiller, B. (2021). SecGrid: A Visual System for the Analysis and

- ML-Based Classification of Cyberattack Traffic. In *IEEE 46th Conference on Local Computer Networks (LCN 2021)*, pages 1–8, Edmonton, Canada.
- Franco, M. F., Granville, L. Z., and Stiller, B. (2023). CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment. In *36th IEEE/IFIP Network Operations and Management Symposium (NOMS 2023)*, pages 1–6, Miami, USA.
- Franco, M. F., Mullick, A. R., and Jha, S. (2024). QBER: Quantifying Cyber Risks for Strategic Decisions. *arXiv preprint arXiv:2405.03513*.
- Gordon, L. A. and Loeb, M. P. (2002a). The Economics of Information Security Investment. *Association for Computing Machinery Transactions on Information and System Security (TISSEC)*, 5(4):438–457. Association for Computing Machinery.
- Gordon, L. A. and Loeb, M. P. (2002b). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 5(4):438–457.
- H. R.K. Skeoch (2021). Expanding the Gordon-Loeb Model to Cyber-Insurance. *Computers & Security*, page 102533.
- Hallman, R., Major, M., Romero-Mariona., J., Phipps, R., Romero, E., and Miguel, J. (2020). Return on Cybersecurity Investment in Operational Technology Systems: Quantifying the Value That Cybersecurity Technologies Provide after Integration. In *5th International Conference on Complexity, Future Information Systems and Risk (COMPLEXIS 2020)*, pages 43–52, Prague, Malta.
- Huang, Y., Debnath, J., Iorga, M., Kumar, A., and Xie, B. (2019). CSAT: A User-interactive Cyber Security Architecture Tool based on NIST-compliance Security Controls for Risk Management. In *IEEE 10th Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, pages 0697–0707, New York, USA.
- Huff, P., McClanahan, K., Le, T., and Li, Q. (2021). A Recommender System for Tracking Vulnerabilities. In *16th International Conference on Availability, Reliability and Security (ARES 2021)*, pages 1–7, Vienna, Austria.
- Kianpour, M., Kowalski, S. J., and Øverby, H. (2021). Systematically Understanding Cybersecurity Economics: A Survey. *Sustainability*, 13(24).
- L. A. Gordon, M. P. Loeb, L. Zhou (2021). Information Segmentation and Investing in Cybersecurity. *Journal of Information Security*, 12:115–136.
- Li, T., Convertino, G., Tayi, R. K., and Kazerooni, S. (2019). What Data Should I Protect? Recommender and Planning Support for Data Security Analysts. In *24th International Conference on Intelligent User Interfaces (IUI '19)*, page 286–297, California, USA.
- Rea-Guaman, M., Calvo-Manzano, J. A., and Feliu, T. S. (2018). A Prototype to Manage Cybersecurity in Small Companies. In *13th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–6, Caceres, Spain.
- Sonnenreich, W., Albanese, J., and Stout, B. (2005). Return On Security Investment (ROSI): A Practical Quantitative Model. *Journal of Research and Practice in Information Technology*, pages 239–252.

All links provided above were last accessed on August 2024.