University of Zurich^UZH

BACHELOR THESIS – Communication Systems Group, Prof. Dr. Burkhard Stiller

A Visual Tool for the Analysis of Cybersecurity Investments

Can Inan
Zurich, Switzerland
Student ID: 14-710-453

Supervisor: Muriel Franco, Bruno Rodrigues
Date of Submission: August 17, 2020

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

ifi

Bachelor Thesis
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland
URL: http://www.csg.uzh.ch/

Abstract

As businesses are increasing their digital dependency, they also get more exposed to cyber threats and cybersecurity has become a crucial factor for companies that depend on information systems. Therefore organizations have to be able to implement powerful cybersechurity measures and manage the related risk and cost for the business. If a business doesn't invest correctly in cybersecurity, the impact of common cyber threats, such as ransomware or Distributed Denial-of-Service (DDoS), can be devastating and result in financial losses, reputation damages as well as business shutdowns. However for an organisation it is not always trivial to know how much money to invest in cybersecurity and in which measures because they want to achieve the highest degree on security while keeping the cost as low as possible. The aim of this thesis is therefore to design and develop a visual tool for cybersecurity investments. It provides a risk assessment and countermeasures for different cyber attacks as well as the return on security investment for the different measures.

Acknowledgments

First of all I would like to thank my supervisor, Muriel Franco, for his regular assistance, interesting discussions and very helpful inputs throughout this thesis. It has been a pleasure to work with someone as kind and smart as Muriel.

I would also like to thank my co-supervisor, Bruno Rodriguez for his support and inputs.

Finally, I would also like to thank Prof. Dr. Burkhard Stiller, head of the Communication System Research Group (CSG) at the University of Zurich, for giving me the possibility to write my bachelor's thesis about such an interesting topic.

Contents

Chapter 1

Introduction

In a technological rapidly evolving world where businesses strengthen their digital dependency, they also become more vulnerable to cyberattacks. It is predicted that the damage of cybercrimes will cost the world six trillion dollar every year by 2021, which is exponentially more than the damage caused by natural disaster and more lucrative than the global trade of all illegal drugs combined [3]. Therefore the decision-makers in cybersecurity of companies have to be able to plan powerful protection mechanisms against cybersecurity threats while managing costs and risks associated with the business.

In a scenario where the goal of the major actors is to achieve the highest possible security and safety standards while desiring to minimize the cost, it is crucial to understand all fundamental cybersecurity risks, impacts, and mitigation measures (or the lack of it) [4]. Based on this information it is possible to estimate and decide whether and how much to invest in cybersecurity. Different approaches are available to support decision-makers during the cybersecurity investment process. For instance, one approach to make an overall estimation is the Return Over Security Investment (ROSI)[7] metric. It provides a benchmark to determine when a concrete investment in a cybersecurity measure is recommended in relation to the potential financial loss and reputation damage a possible cyberattack can cause. However, there is still a lack of approaches and platforms that simplifies the process of analyzing, understanding, and planning investments in cybersecurity.

Security investments are generally complex, because harmful activities typically expose vulnerabilities as a result of under investment in cybersecurity [4]. Therefore it is important for decision-makers to get support by a cybersecurity planning tool, which provides an overview of the possible impacts a cyberattack can have and helps to find a proper strategy to handle a possible or imminent threat. For instance, decision-makers should be able to decide if they want to mitigate the risk of an attack proactively and invest in prevention measures or assume the risk, paying for the damage or pass that on to third parties like cyber insurers. It is critical that businesses make the right decisions in regard of cybersecurity investments otherwise the consequences of an attack can be devastating.

Thus, the goal of this thesis is to design and develop a tool related to cybersecurity and its economic aspects. By using such a tool, decision-makers are able to configure parameters (*e.g.,* business sector and type of attack), analyze the risks, and understand the costs (*e.g.,* downtime of business and reputation loss) of a possible attack. Also, the tool provides details of possible prevention measures to mitigate the risk and cost of a cyberattack. For each mitigation measure the tool provides the investment cost and with the help of the ROSI metric an opportunity for the end user whether he/she wants to invest in one or several measures. An intituitive web-based interface is provided to allow the end user to interact with the platform in order to configure and obtain details related to the cybersecurity investment. Furthermore, case studies are conducted to show the feasibility and performance of the tool.

1.1 Thesis Outline

The rest of this thesis is organized as follows. Chapter 2 provides an overview of the most important concepts for the context of the thesis. Next, in Chapter 3, a literature review is presented as related work. Chapter 4 presents the approach, highlighting the user requirements and calculations of the metrics used for the prototype. Then, Chapter 5 introduces the developed prototype and presents the technical details in a technology-wise manner. Next, The evaluation and discussion on limitations are presented in Chapter 6. Chapter 7 concludes and summarize this thesis and finally Chapter 8 provides details on future work to improve the system.

Chapter 2

Background

The following chapter provides the main idea and impact of cybersecurity economics and explains the importance and difficulties of a risk assessment regarding cybersecurity. Two of the biggest cyber threats businesses are exposed to and the possible protection measures against them will be discussed.

2.1 Economics of Cybersecurity

Dealing with cybersecurity is one of the biggest by-products of a more and more interconnected world, which inevitably puts the economic aspects into discussion. The corporate asset value has changed a lot in the past 20 years. Eighty per cent of the value of Fortune 500 companies now includes intellectual property and other intangibles [11]. This increasing ”digitization” of assets comes along with a digitization of corporate risk.

The economics of cybersecurity uses fundamentals of economics for the analysis of cybersecurity problems [9]. It was often assumed that information security only depends on the technical measures, but Anderson and Moore (2006) have defined the problem as follows: 'People have realised that security failure is caused at least as often by bad incentives as by bad design' [13]. This entails that better incentives and understanding of the possible consequences, which is caused by lack of cybersecurity investment, are needed to raise investments in cybersecurity instead of focusing only on technical measures. Therefore it is important to know the economics behind cybersecurity activities. The United States of America (U.S.A) reported in 2018 a predicted costs in regard to malicious cyber activities of around 57 and 109 billion USD for occurrences which happened only in 2016 [17]. These numbers include, next to the financial loss due to the attacks, additionally the expenditures affecting the improvement and upkeep of system security. Gartner [14] confirms the U.S.A estimate, anticipating a cost of 114 billion USD in 2018 and 124 billion USD in 2019, which shows a raise of 8% for only one country. Cost numbers on a global scale are not exact but there are estimates like [15], that assume costs with regard to cybersecurity activities pass 1 trillion USD added up for the five years from 2017-2021 and taking into consideration the increasing number of Internet of Things (IoT) equipment.

2.1.1 Challenges

For an efficient adoption of cybersecurity, there are different economic obstacles, which makes the decision to where and how invest in cybersecurity challenging. These obstacles include: *(a)* externalities faced by the parties, *(b)* information asymmetry, and *(c)* economic incentives. Each one of these obstacles is described below.

- **Externalities:** An externality is when the loss of a single private network owner, due to risk exploitation, has negative affects not only on the private network but also to many different networks of other firms [8]. Because there is not really a possible way to make a firm accountable for the damage to other firms, caused by its own computer system vulnerabilities, full dependence on the market mechanisms to overcome the externalities issue doesn't work [12]. Without government intervention and/or incentives firms will under invest in cybersecurity activities.
- **Information asymmetry:** Information asymmetry is the economic position, where the market players act under the situation of incomplete information [1]. The information system these days is defined by huge amount of data where accuracy and dependability are demanding, if not impossible to define. This problem consists above all in the assessment of the cost of cybercrime, which are challenging to make because of the lack of data and non reporting due to fear of revealing systematic vulnerabilities or fear of reputational damage [12]. Which has the consequence that the market players are probably not investing enough money and not in the right cybersecurity measures.
- **Incentives:** Taking a closer look to economic incentives gives a better comprehension of the market-oriented behaviour and its link to cybersecurity. Companies determine whether or not to publish threats and vulnerabilities within their systems can often be encouraged to do so through legislative incentives, but others can be scared off by publishing threat and vulnerability information because of risks like damage to trust and reputation, risk of liability, and consequences for the financial market [12]. In general if the payoff is positive for an actor it leads to incentives to execute certain actions and on the other hand if the payoff is negative it can follow to a disincentive and may lead to sub optimal decisions.

2.1.2 Risk Assessment

Risk assessment is the process of evaluation, identification, and estimation of the levels of risks involved in a situation, their comparison against benchmarks or standards, and determination of an acceptable level of risk [36] When implementing a cyber security risk assessment, it is critical to be able to assign numeric values to metrics to calculate the predicted loss, which shows the risk an organization is exposed to due to cyber threats. Although risk assessment is driven by real-world investigations and data, it is very difficult do assign accurate values because of the different unpredictabilities involved (*e.g.*, growing threat and vulnerability landscape, human errors) and the general difficulty of assessing risk [2].

To decide if a measure should be implemented or not, common models use a cost-benefit trade investigation which defines whether a certain investment is acceptable and allows to compare the total expected benefits to the total costs and to see if the benefits exceed the total expected cost and by how much [12]. Nonetheless, it is very challenging to estimate the cost and the benefit aspects in cyber security. A company taking on this model has to know all the direct and indirect costs as well the benefits and the benefits have to be higher than the costs.

2.1.3 Return On Security Investment Model (ROSI)

As organisations have to determine how much they want to invest in cyber security and how much cyber security is sufficient, metrics that quantify the benefits and drawbacks of the different investments are useful. The standard Return On Investment (ROI) model is a measure which is used to figure out the efficiency of an investment or to compare the efficiency of various investments [10]. The ROI formula is the following:

$$ROI = \frac{Expected\ Returns - Cost\ of\ investment}{Cost\ of\ investment} \tag{2.1}$$

However, this formula is not suitable for security investments, because security does not generate profits, it rather avoids losses [12]. In other words, when you invest in cyber security, you expect to diminish the risks which threaten your assets. The evaluation of the Return on Security Investment (ROSI) is done by computing how much loss could be prevented through investment in cyber security. The equation for calculating the ROSI is described as following:

$$ROSI = \frac{(Risk\ Exposure * \%\ Risk\ Mitigated) - Solution\ Cost}{Solution\ Cost} \tag{2.2}$$

To define accurate values for the ROSI equation is not an easy task. There is no "standard" model to analyze the financial consequences in regard to cyber security incidents and there also no standardized methods for determining the risk mitigating effectiveness of security measures [18]. Even the methods to define the cost of a security solution can be very different. Methods to quantify the risk exposure are available but the results are not very accurate, therefore for most types of risk, the exposure is defined by statistical data and claims from the past.

The question arises whether there is any use in calculating ROSI if the data is inaccurate. Obviously yes, because there are many industries, which use inaccurate ROI metrics for a long time. The ROSI metric can be very useful for comparing security measures based on relative value, if the method generates repeatable and consistent results [18].

One method to calculate the risk exposure is to multiply the Single Loss Exposure (SLE), which is the estimated cost of a security incident, with the guessed annual rate of occurrence (ARO). The result is the Annual Loss Exposure (ALE).

$$RiskExposure = ALE = SLE * ARO \tag{2.3}$$

To get data about the real cost of a security incident (SLE) is very demanding. The reason for this is that not many companies really analyze security incidents. When a security breach doesn't have a direct influence on the daily business, it usually goes unnoticed. In cases when a breach gets discovered, the organisation is too occupied fixing the problem to think about how much the incidents costs. When the disaster is over, many organisations try their best to hide the incident to protect their image and/or avoid embarrassment.

To quantify the risk mitigation factor of a security measure is also very challenging. A problem is that security doesn't generate something tangible, it rather mitigates loss. If a loss gets prevented the organization probably will never know about. To define the risk mitigation factor it has been made the argument to simply assume that it mitigates 100% of the risk.

However, there are some problems with this assumption. First, over time security measures become less effective as hackers find counter measures against the solutions. Second security measures are dependant on each other and the effectiveness of other solutions will also have a big impact. Finally security solutions are not implemented to their fullest ability because it would have a negative impact on the productivity of the organisations [18].

Thus, it is clear that the cost for a security measure is not simply a price tag [33]. An organisation has to take in consideration that the most security solution create hurdles for employees, which can result in productivity loss. This fact has also to be kept in mind when calculating the ROSI.

2.2 Cybersecurity Threats

As the protection measures an organisation has to take are very dependant on the existing threats, it is it is very important to organizations know which major cyber threats they are exposed to. Therefore, in this chapter, two of the main cyber threats for businesses are explained and different protection measures discussed.

2.2.1 Ransomware

Ransomware is a malware which blackmails it's victims. It demands a fee (ransom) from it's victims in return for giving back access to their device or data [6]. The cost caused by ransomware attacks are increasing, and Cybersecurity Ventures predicts that the global costs will reach up to $20 billion by next year, which is considerably higher than their estimated damages of $11.5 billion in 2019 and $8 billion in 2018 [5].

Attack Strategy

There are small variations between the different ransomware families but they go through very similar attack phases disregarding whether they are locker-ransomware or crypto-ransomware. These phases are the following [19]:

1. Distribution phase: In the first phase the ransomware is packed and delivered into the victims system using different techniques to exploitation techniques like email attachment or drive-by download.

2. Renaissance Phase: In this phase, the ransomware analyzes the environment and gathers information about the victim's system, such as installed programs, OS version and type of platform.

3. Preparation Phase: Ransomware starts looking for resources such as accessibility functions and user files. In the meantime, if the encryption key is not already added to the payload, ransomware retrieves it from the C&C server. A command-and-control (C&C) server is a computer controlled by an attacker which is utilized to send commands to compromised systems and receive stolen data from a target network [20].

4. Hijacking phase: In this phase ransomware is hijacking the victims resources, which were found in the previous phase and encrypts and/or locks them.

5. Extortion phase: When the Hijacking phase is over, a message is shown to the victim demanding for a ransom with payment instructions.

Figure 2.1 shows a graphical overview of the typical steps a ransomware attack has to follow to succeed.

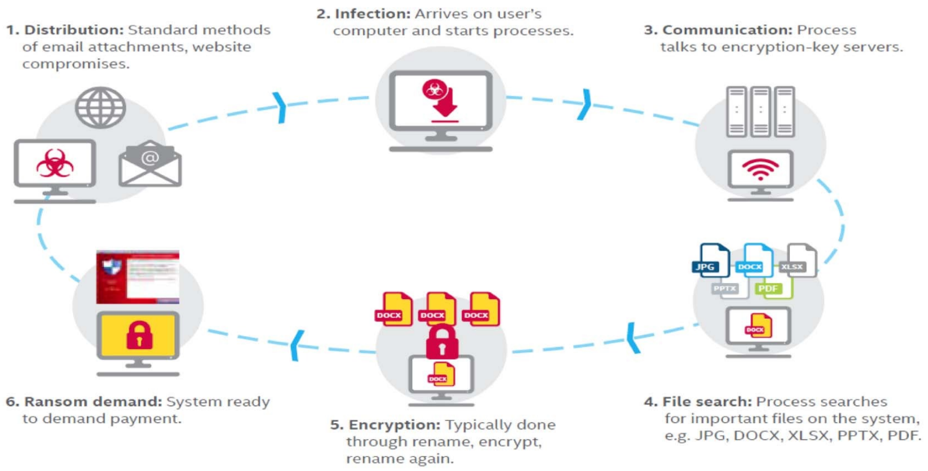

1. Distribution: Standard methods of email attachments, website compromises.
2. Infection: Arrives on user's computer and starts processes.
3. Communication: Process talks to encryption-key servers.
JPG
DOCX
XLSX
PPTX
PDF
DOCX
DOCX
DOCX
DOCX
DOCX
4. File search: Process searches for important files on the system, e.g. JPG, DOCX, XLSX, PPTX, PDF.
5. Encryption: Typically done through rename, encrypt, rename again.
6. Ransom demand: System ready to demand payment.

Figure 2.1: Typical steps of a ransomware attack [21]

Protection

There are different measures to reduce the vulnerability of the system for ransomware attacks which are the following [22].

- **Operation System:** Windows systems have been the most targeted operation system, because many people around the world are using it and when a certain system was target to ransomware attacks before, then most likely is is vulnerable and in high risk of such attacks. It is way safer to have an operation system which is not as commonly used such as Linux. One of the most important measure is to keep the operation system up-to-date because an updated operation system with the latest security updates is more resistant than a non-updated one.
- **Allowed Privileges:** Ransomware are restricted by the allowed privileges given by the operation system. During the installation of the malware, it tries to raise its privileges in different ways; one is pretending to be a normal update asking for administrator privileges [23]. When this privileges are given, mostly by the user, the ransomware infection spreads very easily. To prevent this from happening it is recommended to give users or applications, instead of administrator privileges, restricted privileges such as read only or read and write.
- **Monitoring network:** As mentioned in the chapter Attack Strategy, ransomware are often communicating with a C&C to receive the key to be used while encrypting user files. Therefore, monitoring network traffic, and checking the content of the packets which are received and sent; from and to a device, could be used as an effective defense against ransomware attacks. In addition with monitoring API sequence calls for encrypt, delete or change of the original file or its extension.
- **Backing up data:** Since many types of ransomware are targeting the data of an organisation and encrypt it and use it as leverage, having an up to date back would mitigate the power of the attacker. Some ransomwares can transfer themselves through networks and also infect the data backups. A more secure way is to also have a off-site back up or a secure cloud storage.
- **Storage of the data:** To make it more difficult for ransomware to find important files, storing files in encrypted or encoded format is a way to hide the data.
- **Planning for the unplanned:** In case of an attack happening every organisation should have a disaster recovery plan, which is the last line of defense. This plan includes updated back up of data, employees which are educated and informed about this threat as well as system's ability to reboot and recover from the attack and the possibility to cut down the infected part of the system to get access back.

2.2.2 Distributed Denial-of-Service (DDoS)

A DDoS attack is a type of attack which uses several compromised computer system to target other systems and make them unable to provide normal services to proper users.

Distribution Denial-of-Service (DDoS) attacks are one of the biggest and most damaging cyber threats. The total global estimated number of DDoS attacks are predicted to double to 14.5 Million by 2022, according to the Cisco Visual Networking Index (VNI) of 2017 and the Bulletproof' 2019 Annual Cyber Security Report points out that a DDoS attack could cost up to $120,000 for a small company or over $2 million for an enterprise organization [24].

Attack Strategy

Figure 2.2 shows the basic structure of a DDoS attack. It includes four different components and three different phases . There is an attacker, several control masters and multiple slave components as well as a victim target machine [25]

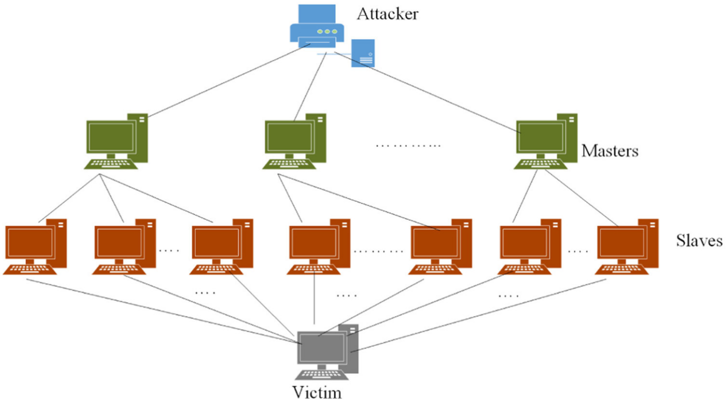


Figure 2.2: Structure of a DDoS attack [25]

In the first phase, the attacker creates a large amount of compromised machines which are the masters and the handlers as they select and control other devices in the attack army. The process to generate a master army is generally automated, where a repeated scanning is done to look for machines with security gaps. With the malicious codes which are installed by the attacker into the masters, it is possible to add more infected machines to the attack army. The slave machines are under direct control of the masters and indirectly controlled by the attacker through these masters [25].

When an acceptable amount of devices have been added to the compromised army, the second phase starts. This compromised army is called a botnet [27]. In the second phase, all the important information such as commands and code is handed over from the attacker to the master armies which pass it on to all slave armies to prepare for the attack [25].

In the last phase, the attacker directs its army to start and carry out attacks. Hence, it sends a huge amount of packets which overwhelms the victim's system. The attacker usually uses fake IP addresses to hide the identity of the compromised devices.

Protection

[28] proposes these measures to reduce the risk of a DDoS attack:

- **Buying more bandwidth:** Having more bandwidth makes the infrastructure more resistant to DDoS attacks because it helps to handle spikes in traffic that are may be caused by malicious activities.

- **Build redundancy into the infrastructure:** To make it difficult to launch a DDoS attack against an organizations servers, it is recommended to spread them across several data centers with a good load balancing system to allocate traffic between them. Ideally they should be in different countries or at least in other regions of the country.

- **Configure network hardware:** Certain simple hardware configuration changes can reduce the risk of a DDoS attack. For instance, configuring the router or firewall to block Domain Name System (DNS) responses or incoming Internet Control Message Protocol (ICMP) packets from outside the organizations network.

- **DDoS protection appliance:** There are many security vendors like Fortinet, NetScout Arbor, Check Point, Radware and Cisco which offer protection appliances that are in front of network firewalls and are created to stop DDoS attacks before happening.

- **DNS server protection:** Malicious actors can bring your DNS server down with a DDoS attack. Because of that it is important that the DNS servers have redundancy and to put them into other data centers behind load balancers. A cloud-based DNS provider which offers bandwidth and several points-of-presence in data centers around the world would be an even better solution.

Chapter 3

Related Work

Due to the constant increase of cyber threats and attacks on organizations over the last decades, cybersecurity has become one of the most important factors, which defines the failure or success of organizations that are dependant on information systems [29]. This fact has led many organizations to take a closer look at cybersecurity investment decisions, particularly to make the right amount of these investments. In the following paragraphs, some frameworks and tools around cybersecurity investment will be discussed.

The ROSI model is described in [18]. which is described to offer a benchmark method to assess the cost/benefit relation of security measures. The authors mention that it is difficult to get accurate data about the cost of security incidents because companies often are not communicating data about security incidents. An other difficulty the authors are talking about is the difficulty of assessing the risk of an organizations system and to determine how much a cybersecurity solution is really mitigating the risk of an attack. Because of this problem, the paper [22] defines for the ransomware use case a value system for the different security measures to determine the vulnerability of the system. This method can also be applied to different cyber threats but to define accurate values for the value system, described in the paper, a lot of research and data is needed.

[4] proposes a framework to determine economic assessments for security measures in complex distributes systems. The framework structures five stages of modelling and mapping, allowing to create economic models based on estimates. To make an economic assessment the framework also uses the ROSI model but it assumes that every measure reduces the risk of an attack by 100%, which of course does not correspond to reality.

Even though there are many studies and papers about cyber security investments but there are not many visual tools available, which analyze the security of an organizations system and provide a risk assessment as well as recommend appropriate security measures and the return on security investment. The aim of the thesis is to deliver a valuable visual tool that provides that.

Chapter 4

Approach

This thesis introduces a visual tool, based on SEConomy framework [4], to help decision-makers during the cybersecurity investment planning. By using the solution, decision-makers are able to set parameters, evaluate their current system and make a risk assessment. Besides that, the solution provides different proactive measures for cyber threats and supports the user with investment decisions related to these measures.

Besides the visual tool, different metrics have been explored to provide details of vulnerabilities and risks. One of the metrics proposed by this work is called Alpha, which represents the vulnerability of the users system in regard to an associated cyber threat. An other one is the Return on Security Investment (ROSI) as mentioned in Chapter 2.1.3, which offers a benchmark to determine when a specific investment in cybersecurity is recommended based on the potential financial loss given an assessed risk.

A functional prototype have been developed in order to show the feasibility of the proposed approach. Details of its implementation are presented in Chapter 5. Also, different case studies (*cf.* Chapter 6) have been conducted in order to show the different flows and discuss the benefits provided by the implemented tool.

4.1 User requirements

To be able to design a visual tool for security investments, it was important to firstly examine the requirements of a decision maker who is going to use the tool. Based on an literature review and analysis of different stakeholders, the following parameters were selected:

- **Threat Type:** This parameter gives information which type of threats the tool covers. The user can choose the type of threat from a drop-down list. Ideally the user has already some knowledge about the existing threats and which threats are most relevant with respect to his organization. So that the user can choose the most important one.

Examples of cyber threats are *Distribution Denial-of-Service*, *Ransomware* and *Phishing.*

- **Business Sector:** The user has to choose in which business sector his organization is. Possible business sectors are for example *Healthcare*, *Finance* and *Information technology.* By choosing a business sector, the tool can provide more accurate information because the cost and risk of an attack are very different for each business sector.
- **Proactive Measures:** After choosing a threat type, the tool provides for the user a drop-down list of possible proactive cybersecurity measures against the selected cyber threat. The user can select one or several measures to get further information about them. Let us assume the user selected, as threat type, a ransomware attack. Some possible proactive measures would be *Access Control*, *Disaster Recovery Plan* or *Data Backup.*
- **Budget:** As the name indicates, the budget parameter defines how much money ($) the user is willing to invest in one or several cybersecurity measures. Once a user has chosen a proactive measure he can define a budget for the measure and the tool will provide the Return On Security Investment (ROSI).
- **System Evaluation:** Dependant on the type of threat the user has selected, the tool will ask different questions about the users system to determine how vulnerable the system is to the chosen threat. For example if the user has chosen, as threat type, a ransomware attack, one question from the system evaluation would be *Type of Operation System?* or *Last time data was backed up?*. It is assumed that the user has knowledge about the current status of his system in use. In the next chapters we will go in more details how the system evaluation works.

These parameters are important in order to present information to the user as precisely as possible. They provide flexibility for decision-maker to compare outputs by setting different parameters. For example, the user can set the parameter *Budget* for various proactive measures to compare the calculated Return on Security Investments, which helps the user to make investment decisions.

4.2 Risk Assessment

As mentioned in Chapter 2.1.2, it is very challenging to make an accurate risk assessment for cybersecurity. There is no standard method and mostly based on research data and past events of cyber incidents. So the methods and data used for the following risk assessment approaches are also based on researched data.

4.2.1 System Evaluation

To make a risk assessment as accurate as possible it is very important to evaluate the systems (*i.e., technology, operating system, and underlying infrastructure*) of the user.

In order to know if the user should invest in cybersecurity, it is important to check how vulnerable the system is to certain threats. If it turns out that the system is already very secure, because in the past the organizations already invested a lot of money into cybersecurity, may no further investment is needed. On the other hand if the evaluation shows that the system is very vulnerable, the user is informed and can invest in cybersecurity.

For every cyber threat included in the tool are the corresponding cybersecurity measures saved in the database. As illustrated in Figure 4.1, every measure has associated submeasures and the submeasures have different options which are also mapped in the database.

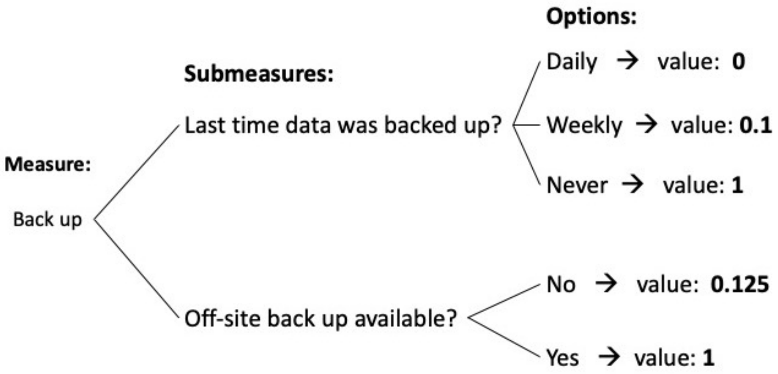


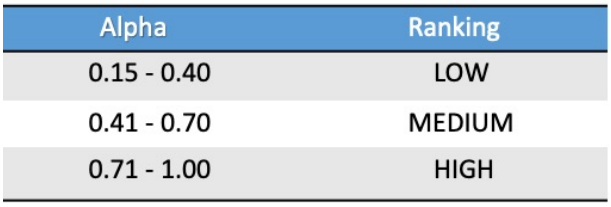
Figure 4.1: System Evaluation mapping example Back up

The submeasures are shown as input parameters and the user can choose one of the associated options in form of a drop-down selection. Every option has an associated weighted value between [0, 1] stored in the database. The weighted value represents how much of an impact the existence or non existence of a cybersecurity measure has on the vulnerability of the system where the number zero represents the highest level of security and one the lowest level. The weight values are based on research and estimates related to a specific cyber threat and are always open for improvement if the state of the research data changes or more data is available.

To calculate the metric for the system vulnerability every weight value (W) is added up and divided by the number of weight values which results in the average weight value for the whole system. We decided to call the metric *Alpha* and the Equation 4.1 below shows the formula to calculate it.

$$Alpha = \frac{(W1 + W2 + W3 + ... + Wn)}{Number\ of\ weight\ values} \quad where\ Alpha \in [0, 1] \tag{4.1}$$

To give context to the calculated number, as illustrated in Table 4.1, *Alpha* is ranked into three different levels. If it is between [0.15, 0.4] the vulnerability of the system is low in relation to a specific cyber attack. On the other hand, if *Alpha* is between [0.41, 0.7] or [0.71, 1] the vulnerability of the system is medium or high, respectively.



Alpha	Ranking
0.15 - 0.40	LOW
0.41 - 0.70	MEDIUM
0.71 - 1.00	HIGH

Table 4.1: Alpha Ranking

4.2.2 Impact of a Cyber Attack

An other important part of the risk assessment is the possible impact of a cyber attack on the organization when a vulnerability gets exploited and an attack would happen. The following metrics are mapped in the database for each cyber threat:

- **Direct Cost:** The direct cost represents the estimated financial consequences in ($) of one associated cyber attack happening and is based on the statistical average cost. It can include for example downtime cost, recovery cost and cost of data loss.
- **Indirect Cost:** Besides the direct cost the indirect costs can not be disregarded. In many cases the indirect costs have an even more severe negative impact on the organization than the direct costs. To quantify the indirect cost is very difficult, because of that we decided to rank it in three stages. There is *Low*, *Medium* and *High* estimated indirect costs. One of these three possibilities is mapped in the database for every cyber threat. In this solution the direct costs are mainly dependant on the affected business sector and are based on statistics and research. The business sector is a key factor how high the indirect costs for an organization are. Examples of indirect costs are loss of reputation and confidence which are for organizations in certain business sectors worse than in others.

4.3 Cybersecurity Investment

This section will discuss the approaches, implemented in the tool to support decision-makers in regard to cybersecurity investment decisions.

4.3.1 Proactive Measures

Security investments are not like other investments, because security does not generate profit, it prevents possible future loss. In order to invest in cybersecurity it is critical to know which measures provide the greatest possible security in the future. So proactive measures are measures taken in the present to prevent greater damage in the future.

As mentioned in section 4.1 the tool provides for the user a drop-down list of possible proactive cybersecurity measures against the selected cyber threat. For every threat are mapped several proactive measure in the database. The different measures are determined based on effectiveness against an associated cyber threat according to research data. To evaluate the system of the user, these measures are divided into submeasures and options, as discussed in section 4.2.1. Cybersecurity insurance, which could also be called a proactive measure, is not used for the system evaluation. Having a cybersecurity insurance doesn't has an influence on the security of the system but it is still mapped in the database as a measure against every threat because it can mitigate the financial loss of an attack and it may be worth investing in it.

4.3.2 ROSI calculation

The metric used in the tool to support the decision making for cyber security investment is based on the ROSI model discussed in chapter 2.1.3. It offers a benchmark to determine when a certain investment in a cybersecurity measure is recommended based on the potential financial loss, mitigation of the risk and the cost of the solution. As shown in the formula 4.2, instead of risk exposure the formula uses the *Direct Cost* which are stored in the database anyway. Of course the *Indirect Cost* should also be a part of the risk exposure but since it is not possible to quantify it, the solution considers only the *Direct Costs.*

$$ROSI = \frac{(Direct\ Cost *\ Risk\ Mitigation\ Factor) - Budget\ for\ the\ measure}{Budget\ for\ the\ measure} \tag{4.2}$$

Cost of solution is replaced with *Budget for the measure*, thus the user can enter how much he is willing to invest in a particular measure. The user himself has to clarify whether it is really possible to carry out the measure with the budget set.

To determine the variable *Risk Mitigation Factor* is challenging, because there is no data available on how much one measure mitigates the risk of an attack. As a solution we used the formula for the *Alpha* (4.1) which represents the system vulnerability. As formula 4.3 shows, *Alpha* is calculated once with and once without the measure and the weight values of all the other measures are kept constant. The difference provides the *Risk Mitigation Factor* of one measure and is mapped in the database for every measure.

$$Risk\ Mitigation\ Factor = Alpha\ with\ Measure\ -\ Alpha\ without\ Measure \tag{4.3}$$

The ROSI metric shows how much (in %) of the cost could be saved by implementing a security measure. In general if the ROSI is positive it is recommended to invest and not if it's negative.

The formula 4.2 calculates the ROSI for one measure, but the tool also provides a ROSI for the case the user wants to invest in several measures as formula 4.4 shows. Direct Costs stay the same but it adds up all the Risk Mitigation Factors *(RMF)* of all the measures the user wants to invest in.

$$ROSI = \frac{(Direct\ Costs * (\ RMF1 +\ RMF2 + .. +\ RMFn) - Total\ Budget}{Total\ Budget} \tag{4.4}$$

Thus, based on the defined use cases and the risk assessment as described, the decision-makers are able to interact with the platform. First, the decision-maker configure the two inputs threat type and business sector. Dependant on these inputs, forms for the system evaluation will be shown to the user. After submitting the forms for the system evaluation, the alpha is calculated and are shown along with the different costs to the user. Next, the user can choose between one or several proactive measure, associated with the cyber attack, set a budget and the tool calculates the Return on Security Investment (ROSI). A graphic that shows the distribution of the targeted business sectors by the chosen threat is also provided.

Chapter 5

Prototype and Implementation

This chapter will offer an overview on the system architecture, technologies, libraries and design used to build the tool.

5.1 Architecture Overview

The proposed tool is implemented based on the components of the MERN stack shown in Fig. 5.1. MERN stands for MongoDB, Express, React and Node which are the four key technologies that make up the stack. The MERN architecture allows to construct a 3-tier architecture (frontend, backend, database) entirely using JavaScript and JSON [30] .

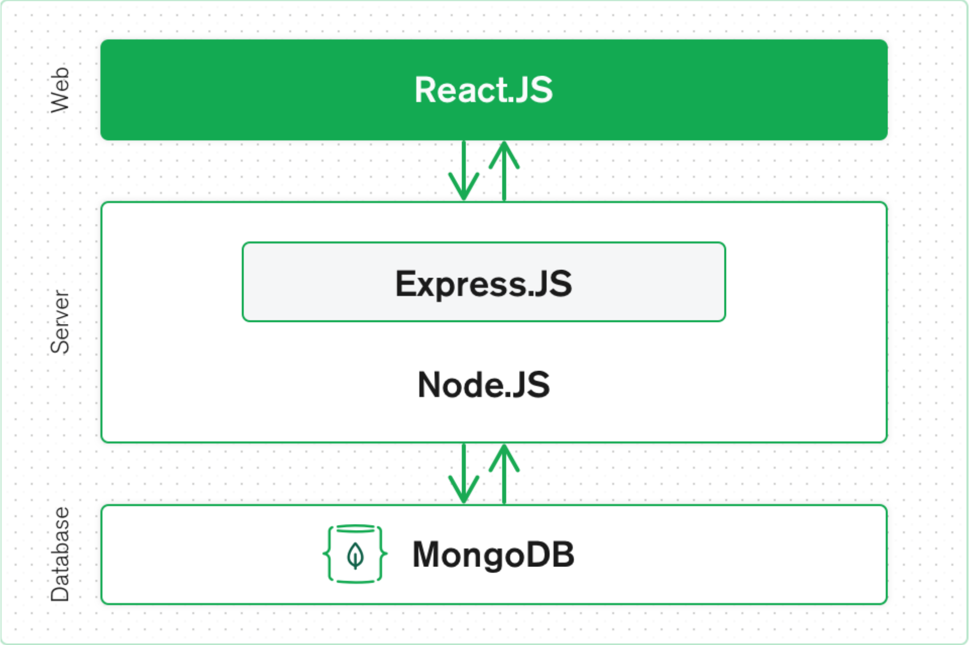


Figure 5.1: Architecture Overview [30]

Calculations of the metrics and communication with the database is handled in the back-end. The user can get access to the platform through any browser and no registration is needed. The client communicates with the server using an Application Programming Interface (API). In the next chapters, we will take a closer look to each component.

5.2 Client

The client-side of the application is implemented using React. React is a very popular Javascript library for creating user interfaces. This library uses so called JSX syntax extension, which facilitates the process of writing UI components. It is easy-to-learn, boosts productivity, facilitates further maintenance and it is backed by a strong community. These are the reasons we decided to use it for building a simple but effective GUI.

5.2.1 User Interface

The tool has an intuitive and dashboard-based design. All the tabs are on one single page as shown in Figure 5.2.

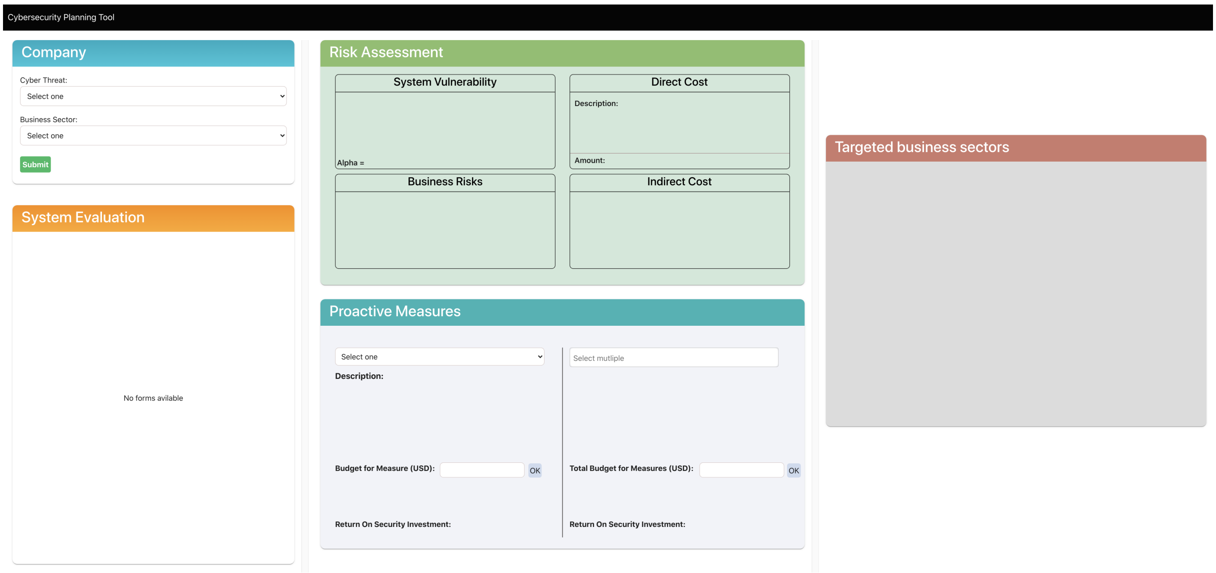
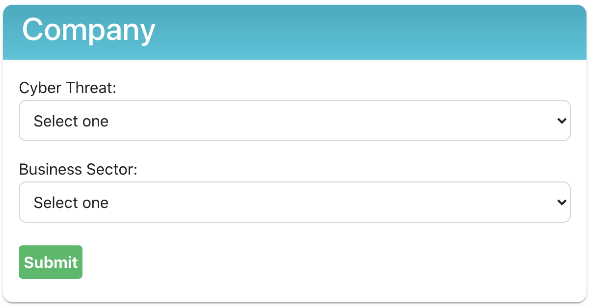


Figure 5.2: Dashboard overview

The system evaluation, risk assessment, proactive measure and targeted business sectors tab have no data available in the beginning, because the data is dependant on the user input in the company tab (Fig. 5.3). In this chapter the user interface is discussed without specific data but in chapter six the tool is evaluated based on a case study and data in different tabs will be shown.

As already discussed in Chapter 4.1 the user can choose in the company tab two different parameters. On the one hand the user has to choose a threat and on the other hand the business sector the organization is in.



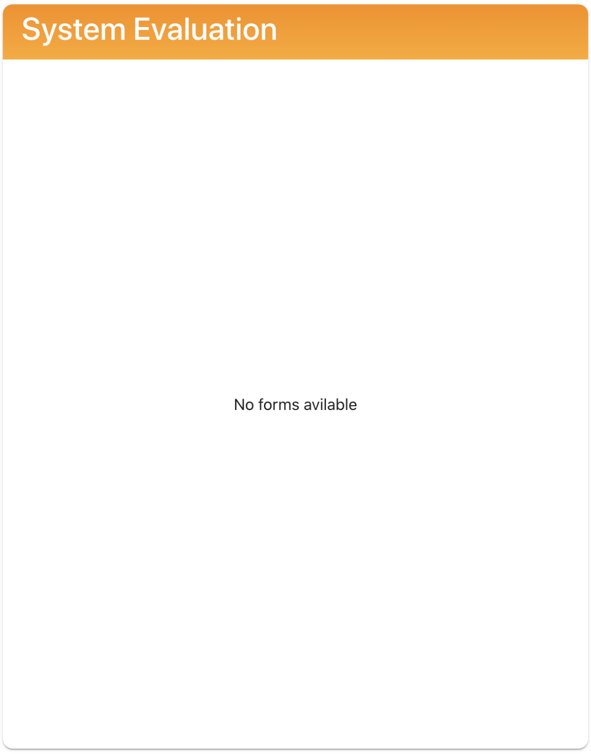
Company

Cyber Threat: Select one

Business Sector: Select one

Figure 5.3: Company Tab

After submitting the data, the back-end will sent the system evaluation forms, associated with the chosen threat, to the client and are shown in the system evaluation tab (Fig. 5.4). As mentioned in Chapter 4.2.1 these forms are needed to evaluate the vulnerability of the system in regard to a certain cyber attack. After choosing an option for every form in the system evaluation tab the user can submit them and the *Alpha*, which represents the system vulnerability, is going to be calculated in the back-end.



System Evaluation

No forms avilable

Figure 5.4: System Evaluation Tab

After the back-end retrieves from the database the different costs, business risks, proactive measure and statistical data, associated with the chosen cyber threat, it is sent together with the calculated *Alpha* to the client.

As shown in Fig. 5.5 the risk assessment tab is split into four different tabs. One tab is the system vulnerability, ranked in *High*, *Medium* or *Low*, which is dependant on the calculated *Alpha*. Other tabs are the direct and indirect costs, which represent the possible impact of a cyber attack as already discussed in chapter 4.2.2. The last tab displays the business risks, showing a list of all the possible consequences an attack could have in more detail.

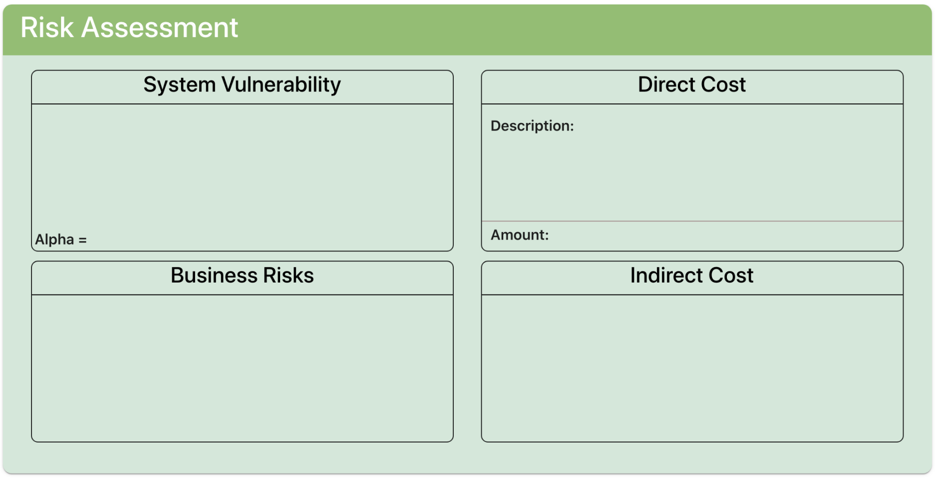


Figure 5.5: Risk Assessment Tab

The proactive measure tap (Fig. 5.6) is an interactive tab. On the left side the user can choose one proactive measure from a drop-down selection and a small description about the measure is shown. Next the user can set a budget on how much he is willing to invest in a certain measure and as soon as the user presses OK the budget is sent to the back-end. In the back-end the return on security investment is calculated and sent to the client and shown to the user. If the user is thinking about investing in several measures, on the right side of the tab the user can choose several measures, set a total budget and calculate the return on security investment.

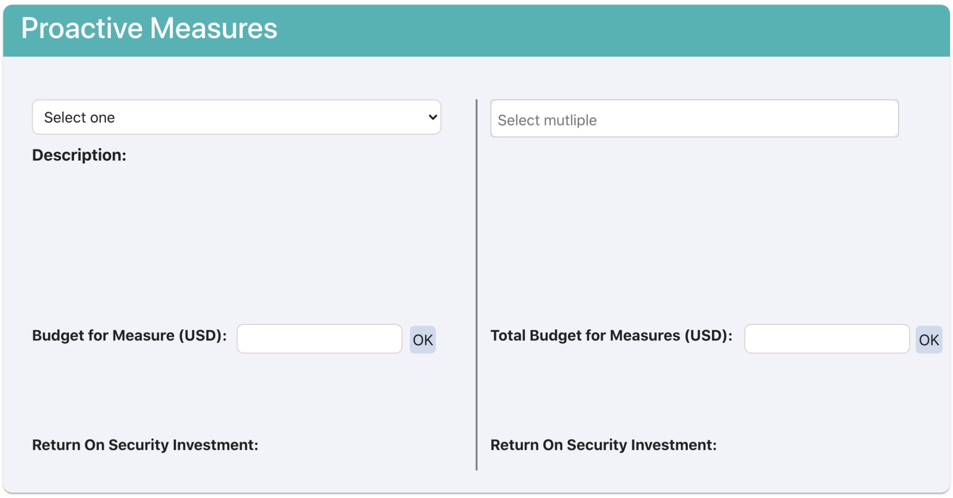

Proactive Measures
Select one
Description:
Budget for Measure (USD):
OK
Return On Security Investment:
Select mutliple
Total Budget for Measures (USD):
OK
Return On Security Investment:

Figure 5.6: Proactive Measures Tab

The last tab (Fig. 5.7) shows a graphic of the targeted business sectors by the chosen threat and it illustrates how badly an industry is affected by it. When the user hovers over a section in the graph, it shows (in %) how many of the the total attacks affect a certain industry. The graphic is implemented with Chart.js, a popular open source JavaScript library for data visualization.

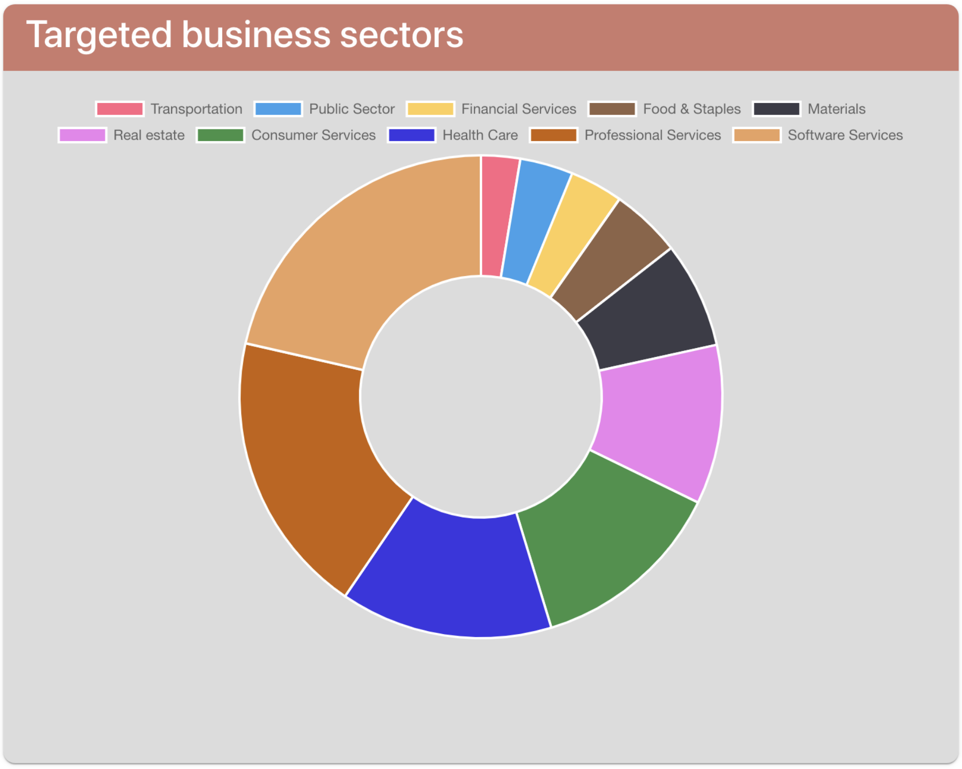


Figure 5.7: Targeted Business Sectors Graphic

5.3 Server

The server-side of our proposed tool is implemented with Node.js and the Express framework. Node.js is a JavaScript runtime built on Chrome's V8 JavaScript engine and it is designed to build scalable network applications [32]. In order to increase performance, the flexible Node.js web application framework Express is used which adds a robust set of features for mobile and web applications [31]. With several HTTP utility methods and a middleware, creating a solid API is simple and quick.

In the context of our prototype the server provides a RESTful API which is an API that uses HTTP requests like GET, PUT, POST and DELETE to allow a communication between endpoints of the server and client side. The user submits data on the client side and sends it to the server more precisely to a specific API endpoint on the server side. The server queries needed data from the database and calculates *i.e.*, the Return On Security Investment and Alpha and sends it to the client.

5.4 Database

The database used for this prototype is MongoDB. MongoDB is a document-oriented database program and classified as a NoSQL database program which uses JSON-like documents with optional schemas, meaning fields can differ from document to document and data structure can be changed over time [34]. It is a distributed database, so horizontal scaling, high availability and geographic distribution are built in. The data for this prototype is stored on MongoDB Atlas which is global cloud database service and very flexible and scalable. In order to establish a database connection, we used a library called Mongoose. Mongoose is a an object data modeling (ODM) library for MongoDB and Node.js. It includes schema validation, handles relationships between data and is utilized to translate between coded objects and the representation of those objects in MongoDB.

Even though MongoDB does not require a strict schema and relations between documents it is still possible to do it. The underlying database schema (Fig. 5.8) represents the database implemented for the prototype.

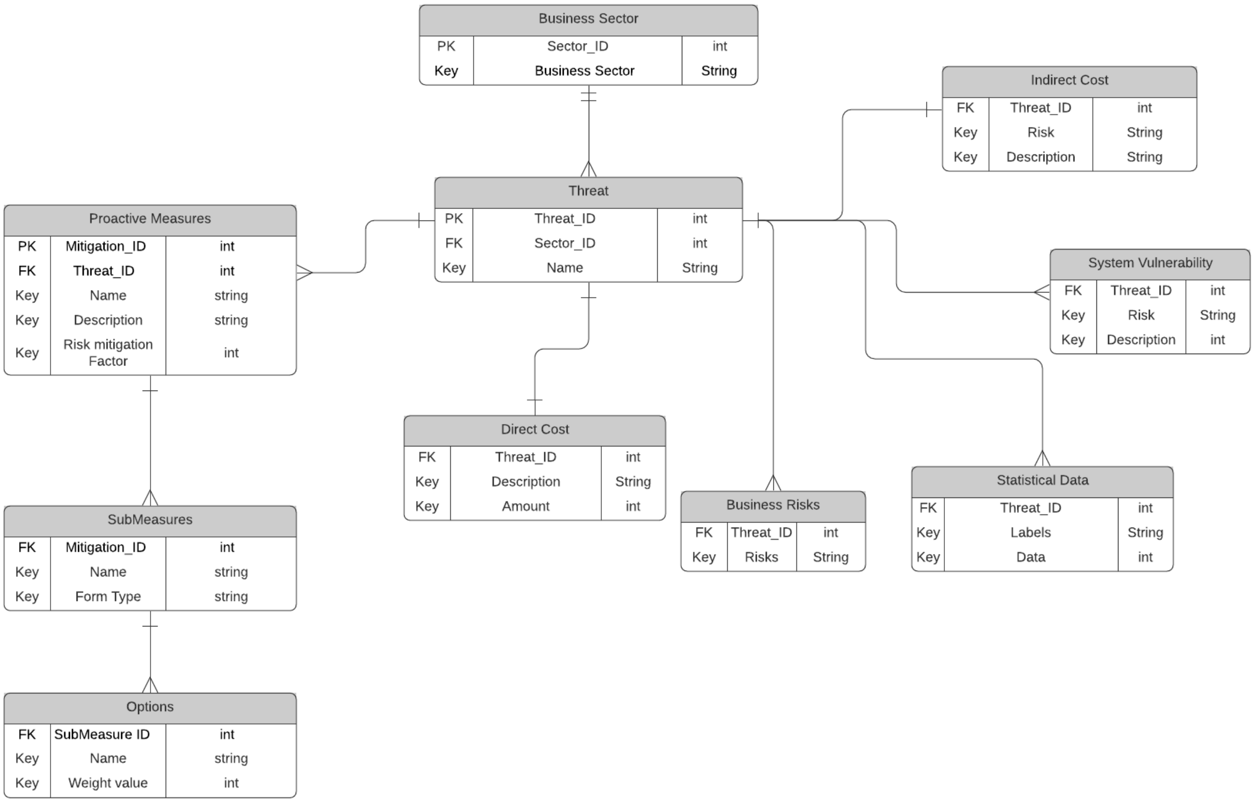


Figure 5.8: Database Schema

In the database is a business sector stored which can have different cyber threats. All the other tables are dependant on the threat. A threat can have different proactive measures, which have submeasures and every submeasure has different options as discussed in chapter 4.2.1. The submeasures and options are stored in the database to send them dynamically as forms to the front-end for the system evaluation. For every cyber threat are also stored the different costs, business risks and the statistical data which is needed for the targeted business sectors graphic (Fig. 5.7). As mentioned in chapter 4.2.2 the data for these metrics are based on research data. Lastly there are mapped for every threat the three possible system vulnerabilities (*Low*, *Medium* or *High*) to the database and get retrieved from the server dependant on the calculated *Alpha*.

Chapter 6

Evaluation

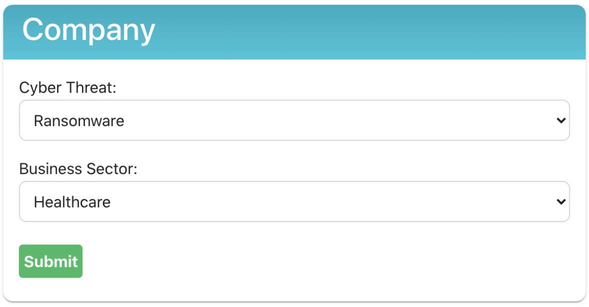
In order to evaluate the usability of the visual tool, the following sections describe two case studies, focusing on two use case scenarios. The case studies aim to cover different features and show the helpfulness of the tool in cybersecurity risk assessment and investment. In the first case study, we will carry out an evaluation of a user's system and the associated cybersecurity risk assessment. In the second one, we discuss some possible investment decisions, based on the risk assessment from Case Study No. 1, by calculating the Return on Security Investment (ROSI). Finally, a discussion, where we analyze the tool's advantages and limitations, is provided.

6.1 Case Study No. 1 - Risk Assessment

For this case study, let us consider the user of the tool is the IT project leader of a hospital. He/She has the responsibility and makes the decisions regarding all the IT. One day, the hospital management approaches the IT project leader and is talking about his concerns regarding the steady increase of cyber attacks lately, especially in the healthcare sector. The user read in the news that many hospitals have to deal with ransomware attacks and some of them suffered much damage from it. The management wants to know from the IT project leader how well prepared respectively how secure their system is concerning ransomware attacks or if the system has to be improved and the possible impact in case of an attack. Keeping that in mind, the IT project leader will use the proposed tool to support him with the given task.

First and foremost, the user will set the two parameters in the company tab (Fig. 6.1). There he can choose a cyber attack and the relevant business sector from a drop-down menu. In this case, the user chooses healthcare as the business sector and ransomware as an attack type.

After submitting the parameters in the company tab, the forms for evaluating the vulnerability of the system in regard to a ransomware attack are shown (Fig. 6.2). In Figure 6.2 the options are set to default values, which represent the worst case respectively the highest vulnerability of the system. Lets assume the user keeps the options like that and

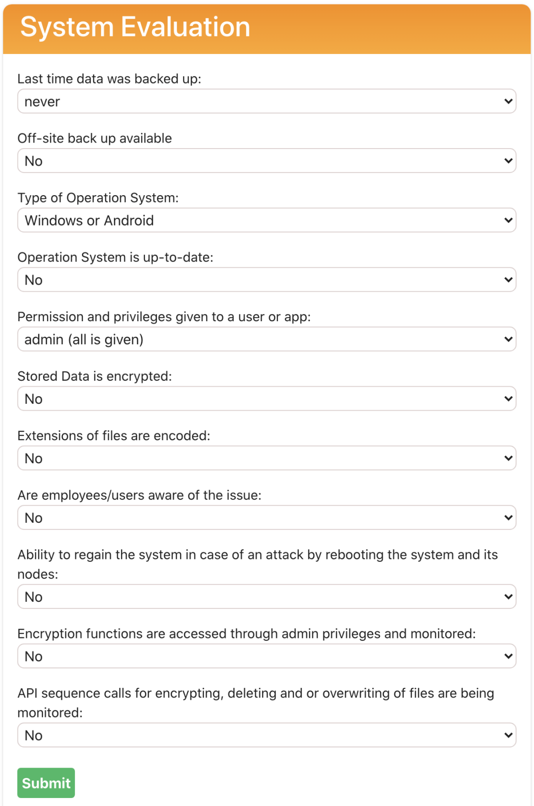


Cyber Threat: Ransomware

Business Sector: Healthcare

Figure 6.1: Company Tab

this would be an accurate representation of the hospitals system. By calculating the *Alpha* of the system by applying equation 4.1, therefor $Alpha = 1$ for this case. This would mean that the system of the hospital is highly vulnerable for ransomware attacks and in the past have never been made any investments in cybersecurity measures. As a consequence it is highly advised to inform the management of the hospital about the lack of security and a budget for cybersecurity investment should be provided.



Last time data was backed up: never

Off-site back up available: No

Type of Operation System: Windows or Android

Operation System is up-to-date: No

Permission and privileges given to a user or app: admin (all is given)

Stored Data is encrypted: No

Extensions of files are encoded: No

Are employees/users aware of the issue: No

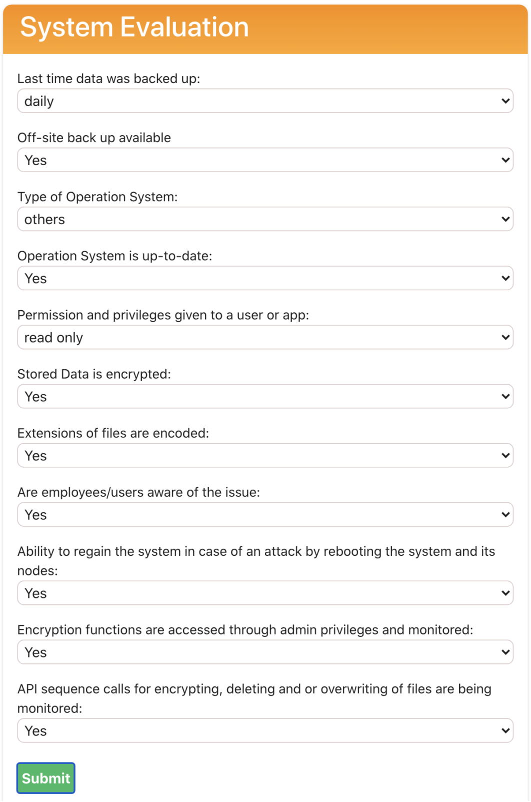
Ability to regain the system in case of an attack by rebooting the system and its nodes: No

Encryption functions are accessed through admin privileges and monitored: No

API sequence calls for encrypting, deleting and or overwriting of files are being monitored: No

Figure 6.2: System Evaluation Tab Ransomware (worst case)

Now, let us look at the opposite and assume the hospital has already a very secure system and is well prepared against ransomware attacks. The user selects this time in the system evaluation tab (Fig. 6.3) for every form the best possible option and therefore $Alpha = 0.19$ for this case. The result is not as one might believe $Alpha = 0$, because the system is even with the highest security standards not one hundred percent secure against an attack. This represents the best case scenario of the hospitals system and it means that the hospital in the past has already invested in all the measures to improve the system. The only thing the user could suggest to the management is to invest in cyber insurance if not already existing.



System Evaluation

Last time data was backed up: daily

Off-site back up available: Yes

Type of Operation System: others

Operation System is up-to-date: Yes

Permission and privileges given to a user or app: read only

Stored Data is encrypted: Yes

Extensions of files are encoded: Yes

Are employees/users aware of the issue: Yes

Ability to regain the system in case of an attack by rebooting the system and its nodes: Yes

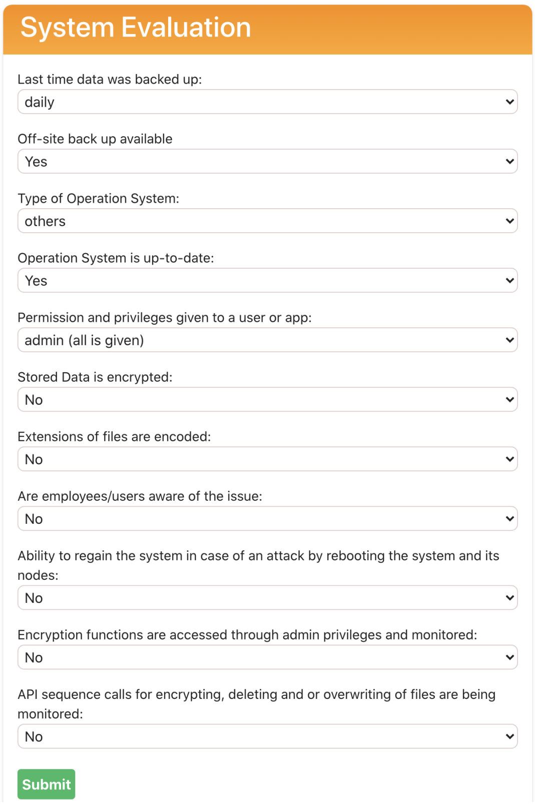
Encryption functions are accessed through admin privileges and monitored: Yes

API sequence calls for encrypting, deleting and or overwriting of files are being monitored: Yes

Figure 6.3: System Evaluation Tab Ransomware (best case)

Lastly, let us take a more realistic case and assume that the hospital already has daily back up, off-site back is available and has a secure operating system as well the operating system is kept up to date. However, all the other measures are not provided. The system evaluation in Figure 6.4 shows this scenario. Let us assume that this represents the actual system of the hospital regarding our case study. The IT project leader selects the forms accordingly and submits them.

After submitting them, the data is shown in all the other tabs. Also, the risk assessment tab with the data (Fig. 6.5) is shown, which provides the *Alpha* respectively the system vulnerability, direct cost, indirect cost and business risks as already discussed in chapter 5.2.1 As shown in Figure 6.5 the *Alpha*, in this case, is 0.69 which represents according to the alpha ranking in Table 4.1 in chapter 4.2.2 a *Medium* vulnerability of the system. It means that the system is not highly vulnerable, but it can still be improved. On the upper right tab (Fig. 6.5), the user can see the possible financial impact of a ransomware attack in healthcare, which is $ 120,000. Besides, he/she can see that the indirect cost would be *High*, because of the reputation damage and confidence loss of the hospital. The targeted business sectors tab (Fig. 6.6) also provides useful information for the risk assessment. When the user hovers over the healthcare sector of the graph, it shows the number 13.6 %,



System Evaluation

Last time data was backed up:
daily

Off-site back up available
Yes

Type of Operation System:
others

Operation System is up-to-date:
Yes

Permission and privileges given to a user or app:
admin (all is given)

Stored Data is encrypted:
No

Extensions of files are encoded:
No

Are employees/users aware of the issue:
No

Ability to regain the system in case of an attack by rebooting the system and its nodes:
No

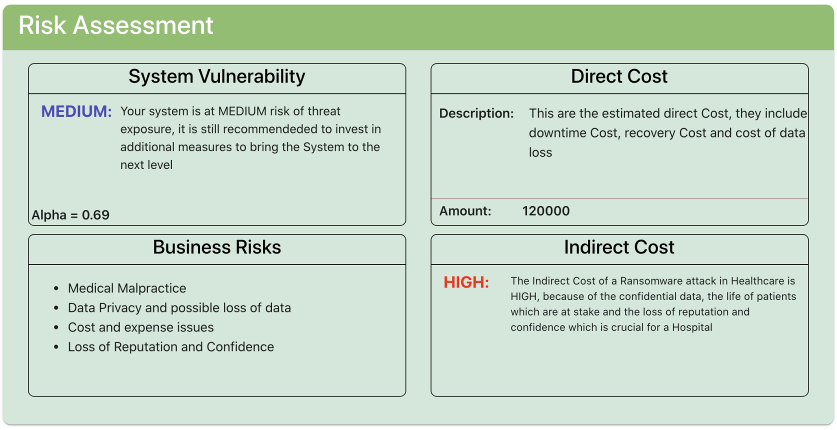
Encryption functions are accessed through admin privileges and monitored:
No

API sequence calls for encrypting, deleting and or overwriting of files are being monitored:
No

Figure 6.4: System Evaluation Tab Ransomware (medium case)

which tells the user that 13.6 % of all the ransomware attacks are targeting the healthcare sector. Thus the healthcare sector is the third biggest sector in the graphic.

With all this information, the IT project leader can go to the management and provide some useful information about the current system's security and the possible impact a ransomware attack could have. This information provides a good foundation for cybersecurity investment decisions and the management can decide whether they want to provide a budget to invest in additional measures.



Risk Assessment

System Vulnerability

MEDIUM: Your system is at MEDIUM risk of threat exposure, it is still recommendeded to invest in additional measures to bring the System to the next level

Alpha = 0.69

Direct Cost

Description: This are the estimated direct Cost, they include downtime Cost, recovery Cost and cost of data loss

Amount: 120000

Business Risks

- Medical Malpractice
- Data Privacy and possible loss of data
- Cost and expense issues
- Loss of Reputation and Confidence

Indirect Cost

HIGH: The Indirect Cost of a Ransomware attack in Healthcare is HIGH, because of the confidential data, the life of patients which are at stake and the loss of reputation and confidence which is crucial for a Hospital

Figure 6.5: Risk Assessment Tab Ransomware (medium case)

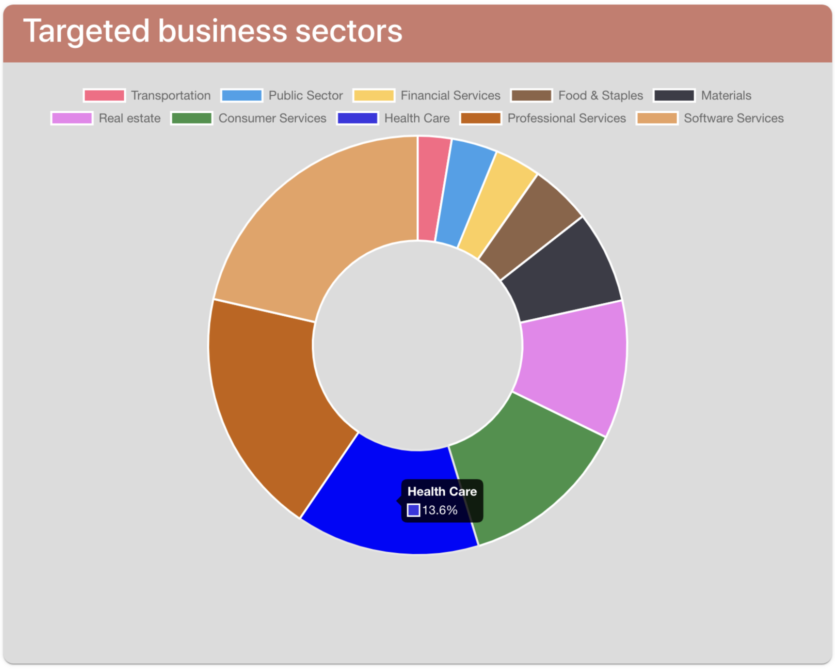
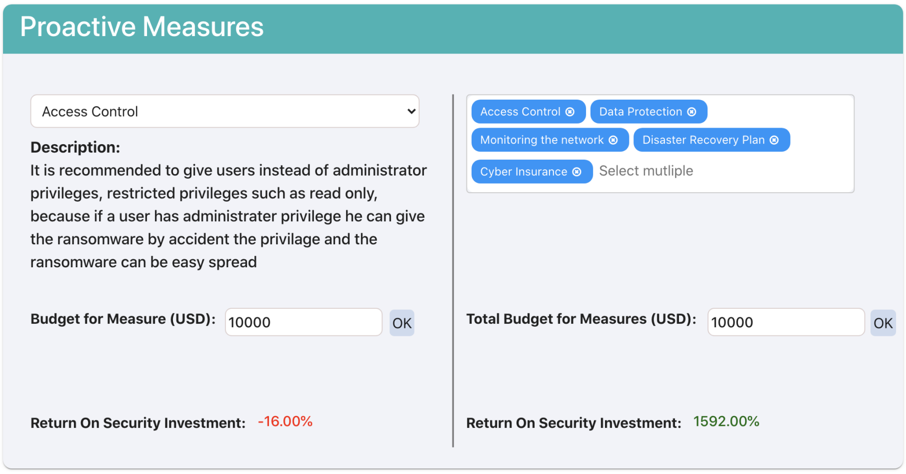


Figure 6.6: Targeted business sectors by Ransomware

6.2 Case Study No. 2 - Investment Decisions

For this case study, let us assume the hospital's management team decides, after seeing the data presented in Case Study No. 1, to improve the security of the system against ransomware attacks. The management provides a budget of $ 10,000 and advises the IT project manager that he should invest the budget in order to provide the highest Return On Investment. To help the user by making cybersecurity investment decisions, the tool provides, as discussed in chapter 5.2.1, the proactive measure tab (*cf.*, Fig 6.7).



Proactive Measures

Access Control

Description:
It is recommended to give users instead of administrator privileges, restricted privileges such as read only, because if a user has administrater privilege he can give the ransomware by accident the privilage and the ransomware can be easy spread

Budget for Measure (USD): 10000 OK

Return On Security Investment: -16.00%

Access Control ⊗ Data Protection ⊗ Monitoring the network ⊗ Disaster Recovery Plan ⊗ Cyber Insurance ⊗ Select mutliple

Total Budget for Measures (USD): 10000 OK

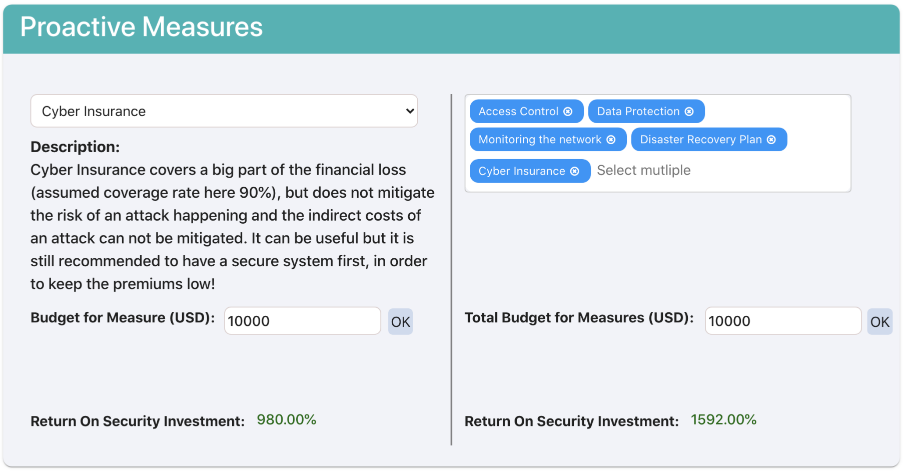
Return On Security Investment: 1592.00%

Figure 6.7: Proactive Measures Ransomware

On the left side of the proactive measure tab, the user can choose one measure against ransomware, read the description of the measure, set the budget, and calculate the Return

On Security Investment (ROSI). In Figure 6.7, the user chose the measure Access Control, which is one of the measures not provided in the hospital system yet. If he/she sets the total budget of $ 10,000 for only this measure, the tool calculates a ROSI of -16.00 %. This means that if the implementation of the measure Access Control would cost $ 10,000 and thus use up the whole budget, it is not advised to invest in the measure.

Let us look at a second measure shown in Figure 6.8 on the left side of the tab. At this time, the user chooses Cyber Insurance as a measure with an assumed coverage rate of 90 % and sets the budget again on $ 10,000. The calculate Return on Security Investment is 980 % and it would be advised to invest in Cyber Insurance.



Proactive Measures

Cyber Insurance

Description:
Cyber Insurance covers a big part of the financial loss (assumed coverage rate here 90%), but does not mitigate the risk of an attack happening and the indirect costs of an attack can not be mitigated. It can be useful but it is still recommended to have a secure system first, in order to keep the premiums low!

Budget for Measure (USD): 10000 OK

Return On Security Investment: 980.00%

Access Control ⊗ Data Protection ⊗ Monitoring the network ⊗ Disaster Recovery Plan ⊗ Cyber Insurance ⊗ Select mutliple

Total Budget for Measures (USD): 10000 OK

Return On Security Investment: 1592.00%

Figure 6.8: Proactive Measures Ransomware

On the right side of the proactive measures tab (Fig. 6.7 & 6.8) the user can choose several measures and set a budget and calculate the ROSI. The user selects as shown in Figure 6.8 all the additional proactive measure that the hospital does not have and sets the total budget of $ 10,000 and the tool provides the ROSI of 1592 %. This means that if it is possible to implement all these measures with the budget of $ 10,000 it would be highly advised to invest in all the missing measures.

The IT project manager can inform the management that investing in all these measures would provide the highest ROSI but first, they have to clarify how much it would cost to implement these solutions for the hospital in order to verify if it is possible with the set budget. If it is not possible, they either have to increase the budget or implement fewer measures.

6.3 Discussion

The two case studies deal with the two different main concepts provided by the tool. Both the risk assessment and the investment in cybersecurity aim to be simplified in the proposed solution. The critical information is provided to the user with a graphical and interactive user interface for the cybersecurity risk assessment and investment. The user gets an idea of the risk his organization is exposed to and possible investment strategies he/she could implement.

One of the tool's limitations is that the user can only choose one cyber threat at the time and has to do the cybersecurity risk assessment and investment separately for every threat. If the user were able to choose several threats at once, it would make the tool a lot more complicated because the system evaluation would be very long. The user had to select forms for every threat and a dependency between the different cyber attacks. The risk of one cyber threat has an impact on the risk of another one, and there is a possible cascade failing, which is not considered in the tool.

Another limitation of the tool is the accuracy. The mapping of the different weight values for the system evaluation is dependent on research, and it is challenging to define them so that they represent reality because the research data is limited. The tool depends on the weight values because they are used to calculate the *Alpha* and the *Risk Mitigation Factor*, which has a significant impact on the accuracy of the ROSI metric. Also, the accuracy of the direct cost and indirect cost is dependant on the research data. If the data is not available, it is not possible to make an accurate risk assessment.

As shown in Case Study No. 2, the user has to find out how much the implementation of specific security measures would cost. If there would be accurate data available on how much it costs to implement specific measures, they could be mapped to the database and the user has only to set the budget without doing any research about the cost of the measures. At the moment, the user's set budget represents the cost of the associated measure because of the lack of available data.

Chapter 7

Summary and Conclusions

As businesses strengthen their digital dependency, they also become more vulnerable to cyberattacks, which inevitably puts the economic aspects into discussion. Hence the demand for tools to support businesses in cybersecurity decisions is increasing. The main objective of this thesis was to design and develop a visual tool for the analysis of cybersecurity investments to support the user in the decision-making process.

After having set out the introduction and motivation, some theoretical background is given on cybersecurity economics, risk assessment and two common cyber threats, businesses are frequently exposed to, were analyzed. With this background in mind, related work in the same field of research is discussed. In the next chapter the approach of the tool is presented by defining the user requirements and discussing the different metrics and calculations used by the visual tool. The following chapter tackled implementation topics such as the design of the user interface and the client-server architecture as well as the technologies, libraries and programming language used to develop the tool. Further, an evaluation of the proposed visual tool is conducted based on two different use case scenarios and followed by a discussion of the prototype. Possible extensions of the tool are then set out in the *Future Work* section.

The proposed prototype is able to analyze the security of an organizations system, regarding an associated cyber attack, provide a risk assessment and recommend appropriate security measures and the Return On Security Investment (ROSI). Although the tool has its limitations, the implementation especially of the database offers wide extensibility and we could imagine a whole bunch of appendices into the platform, achieving an even richer application.

Chapter 8

Future Work

One of the firs steps in the future is to add more data to the database for different cyber attacks and business sectors to provide a wider selection for the user which makes the tool more complete. Since the database can be easily expanded, it is not a difficult task if the data is available. The possibility for the user to select several cyberattacks at the time, enabling an overall cybersecurity assessment, which also considers the dependencies between different cyber threats, would be a useful additional feature to implement in the future. The user profile could also be expanded by adding more parameters to make the risk assessment especially the direct and indirect cost more accurate and tailored to the individual users organization. Furthermore adding an existing protective recommender system like MENTOR [33], could add a lot of value to the tool by improving the quality and accuracy of the provided security measures.

Future work will also focus on investigating different machine learning and data mining techniques to improve data accuracy and quality as well as automate the storage of new data in the database. Additional future studies should investigate the possibility of recommending cybersecurity investments on an automated basis when the research data changes or new vulnerabilities were discovered.

Bibliography

[1] A.Bloomenthal: *Asymmetric Information*, https://www.investopedia.com/terms/a/asymmetricinformation.asp, (last accessed July 2020).

[2] A. Fielder, S. Koenig, E. Panaousis, S. Schauer, S. Rass: *Risk Assessment Uncertainties in Cybersecurity Investments*, 2018.

[3] S.Morgan: *2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics*, https://cybersecurityventures.com/cybersecurity-almanac-2019/, (last accessed Mai 2020).

[4] B.Rodrigues, M.F.Franco, G.Pranghi, B.Stiller: *SEConomy: A Framework for the Economic Assessment of Cybersecurity; 16th International Conference on the Economics of Grids, Clouds, Systems, and Services (GECON)*, 2019.

[5] C. Crane: *20 Ransomware Statistics You are Powerless to Resist Reading*, https://www.thesslstore.com/blog/ransomware-statistics, (last accessed July 2020).

[6] G. Hull, H. John, B. Arief: *Ransomware deployment methods and analysis: views from a predictive model and human responses*, February, 2019.

[7] G.Morates: *Things to Consider When Calculating the Return on Security Investment*, https://securityintelligence.com/thing-to-consider-when-calculating-the-return-on-security-investment/, (last accessed Mai 2020).

[8] L.A. Gordon, M.P. Loeb, W. Lucyshyn, L. Zhou: *Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model*, Journal of Information Security, 2015.

[9] IPACSO: *State-of-the-art of the Economics of Cyber-security and privacy*, http://ipacso.eu/downloads/public-deliverables.html (last accessed July 2020).

[10] J.Chen: *Return on Investment (ROI)*, https://www.investopedia.com/terms/r/returnoninvestment.asp, (last accessed July 2020).

[11] L. Clinton: *5 economic principles of cyber security*, https://www.weforum.org/agenda/2015/02/5-economic-principles-of-cyber-security/, (last accessed July 2020).

[12] P. Brangetto, M. K. Aubyn: *Economic aspects of national cyber security strategies*, 2015.

[13] R. Anderson, et al.: *The Economics of Information Security*, Science, 2006.

[14] S. Moore: *Gartner Forecasts Worldwide Information Security Spending to Exceed 124 Billion in 2019*, https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019, (last accessed July 2020).

[15] S. Morgan: *2019 Official Annual Cybercrime Report*, Herjavec Group, 2019.

[16] T.Moore: *The economics of cybersecurity: Principles and policy options*, 2010.

[17] WhiteHouse: *The Cost of Malicious Cyber Activity to the U.S. Economy*, 2018.

[18] W. Sonnenreich, J. Albanese, B. Stout: *Return On Security Investment (ROSI): A Practical Quantitative Modell*; Journal of Research and Practice in Information Technology, 2005.

[19] B. Al-rimy, M. A. Maarof, S. Shaid: *Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions*, January, 2018

[20] Trendmicro: *Command and Control Server*, `https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server`, (last accessed July 2020).

[21] McAfee Labs: *Understanding Ransomware and Strategies to Defeat it*, March, 2016.

[22] R. Malkawe, M. Qasaimeh, F. Ghanim, M. Ababneh: *Toward an Early Assessment for Ransomware Attack Vulnerabilities*, 2019

[23] M. P. Zavarsky, D. Lindskog: *Experimental Analysis of Ransomware on Windows and Android Platforms-Evolution and Characterization*, 2016

[24] C.Crane: *The 15 top DDoS statistics you should know in 2020*, `https://cybersecurityventures.com/the-15-top-ddos-statistics-you-should-know-in-2020/`, (last accessed August 2020)

[25] T. Mahjabin, Y. Xiao, G. Sun, W. Jiang: *A survey of distributed denial-of-service attack, prevention, and mitigation techniques*, 2017

[26] C. Douligeris, A. Mitrokotsa: *DDoS attacks and defense mechanisms: classification and state-of-the-art*, 2004

[27] S. Coggeshall: *What is a distributed denial of service attack (DDoS) and what can you do about them?*, `https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html`, (last accessed August 2020)

[28] P. Rubens: *How to prevent DDoS attacks: 6 tips to keep your website safe*, https://www.esecurityplanet.com/network-security/how-to-prevent-ddos-attacks.htmlf, (last accessed August 2020)

[29] M. Chronopoulos, E. Panaousis, J. Grossklags: *An options Approach to Cybersecurity Investment*, 2017

[30] MongoDB: *MERN Stack*, https://www.mongodb.com/mern-stack, (last accessed August 2020)

[31] Express: *Express*, https://expressjs.com/, (last accessed August 2020)

[32] Nodejs: *Nodejs*, https://nodejs.org/en/, (last accessed August 2020)

[33] M. F. Franco, B. Rodrigues and B. Stiller: *MENTOR: The Design and Evaluation of a Protection Services Recommender System; 15th International Conference on Network and Service Management (CNSM)*, Halifax, NS, Canada, 2019.

[34] MongoDB: *What is MongoDB*, https://www.mongodb.com/what-is-mongodb, (last accessed August 2020)

[35] freeCodeCamp: *Introduction to Mongoose for MongoDB*, https://www.freecodecamp.org/news/introduction-to-mongoose-for-mongodb-d2a7aa593c57/, (last accessed August 2020)

[36] BusinessDictionary: *Risk Assessment*, http://www.businessdictionary.com/definition/risk-assessment.html, (last accessed August 2020)

Abbreviations

ROSI	Return On Security Investment
IOT	Internet Of Things
ROI	Return On Investment
SLE	Single Loss Exposure
ARO	Annual Rate of Occurrence
ALE	Annual Loss Exposure
C&C	Command and Control
API	Application Programming Interface
DDoS	Distributed Denial-of-Service
VNI	Visual Networking Index
DNS	Domain Name System
ICMP	Internet Control Message Protocol
W	Weight Value
RMF	Risk Mitigation Factor
MERN	MongoDB, Express, React and Node
JSON	JavaScript Object Notation
UI	User Interface
GUI	Graphical User Interface
REST	Representational state transfer
HTTP	Hypertext Transfer Protocol
ODM	Object Data Modelling

List of Figures

List of Tables

Appendix A

Installation Guidelines

This chapter provides the necessary information to install and run the prototype of the tool on a computer with a installation of Apple's macOS. The set up for an other operating system should work very similar. The source code of the prototype is available on Github or Gitlab of the Institute of Informatics at the University of Zurich.

1. **Initial Setup:**

   First the installation of the Node Package Manager (npm) is necessary. It comes along with the *Node.js* and can be installed from the website: `https://www.npmjs.com/get-npm`

2. **Clone Github Repository**

   (a) Download Visual Studio Code (or any *IDE* of your preference): `https://code.visualstudio.com/`

   (b) Open Visual Studio Code and click *Clone Repository*

   (c) As URL copy and paste the following url: `https://github.com/cinan93/CyberSecurityInvestmentTool.git` and change the directory if needed

3. **Starting the application**

   (a) First open the terminal and navigate into the directory of the source code.

   (b) Go to the server folder by executing the following command *$ cd server*, next all the necessary node packages defined in the *packages.json* file need to be installed by running the following command through the Command-Line Interface (CLI): *$ npm install*

   (c) Start the server with the command: *$ npm run dev*

   (d) Open a new terminal and make sure you are in the folder of the application, this time execute the command *$ cd client* and again install the necessary packages with the *$ npm install* command.

   (e) Start the client with the command: *$ npm start*

   (f) The application will be running on *localhost: 3000*

Appendix B

Contents of the CD

- Source code of the application (client and server)
- Final thesis (PDF) and the LaTex source code
- Intermediate presentation (PDF)
- Final presentation (PDF)