NOVA IMS Information Management School

MGI

Mestrado em Gestão de Informação
Master Program in Information Management

# DESIGN OF A SECURITY TOOLBOX:
## A FRAMEWORK TO MITIGATE THE RISKS OF CYBERSPACE

Nuno Miguel de Almeida Farelo

Dissertation presented as partial requirement for obtaining the Master's degree in Information Management, with specialization in Information Systems and Technologies Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

**NOVA Information Management School**
**Instituto Superior de Estatística e Gestão de Informação**
Universidade Nova de Lisboa

# DESIGN OF A SECURITY TOOLBOX: A FRAMEWORK TO MITIGATE THE RISKS OF CYBERSPACE

by

Nuno Miguel de Almeida Farelo

Dissertation presented as partial requirement for obtaining the Master's degree in Information Management with a specialization in Information Systems and Technologies Management

**Advisor:** *Vítor Duarte dos Santos*

**Advisor***: Henrique Mamede*

November 2022

# ABSTRACT

This research aims to create a framework that helps SMEs mitigate the various risks of cyberspace. In this digital era, the dangers of cyberspace are increasing, which leads to the need for organizations to adopt adequate security measures capable of preventing cyberattacks. However, a large number of employees in SMEs do not know how to act to mitigate the risks already mentioned. Thus, the development of a security toolbox could be a solution to help SMEs be less exposed to the dangers of cyberspace.

For this research, a theoretical overview associated with cybersecurity to understand the current state of security solutions and the different control options in the organizational environment was essential. Last but not least, a clear understanding of the SMEs needs, in the area of security, was also crucial in the development and construction of the proposed artifact. To evaluate and validate the security toolbox, focus group meetings will be scheduled.

The implementation of a security toolbox that helps SMEs to identify, protect, respond and recover from potential cyberattacks, may be relevant and can provide great results for different organizational environments to mitigate the risks of cyberspace. The suggested framework would play an important role, to the users of the security Toolbox to get more know-how to protect the business environment. Also, may be seen as a vantage to the science since will help to develop the research related to improving the techniques and tools disposal to mitigate the high risks of cyberspace.

# KEYWORDS

Cybersecurity; SMEs; Security Architecture; Cyberspace; Information Security

# INDEX

# INDEX OF FIGURES

# INDEX OF TABLES

# LIST OF ABREVIATTIONS AND ACRONYMS

AI – Artificial Intelligence

CIA - Confidentiality, Integrity and Availability

DoS – Denial of Device

DSR – Design Science Research

DSRM – Design Science Research Methodology

ENISA – European Union Agency for Cybersecurity

GCA - Global Cyber Alliance

ISO/ IEC – International Organization for Standardization / International Electrotechnical Commission

IT – Information Technology

ML – Machine Learning

NIST – National Institute of Standards and Technology

PRISMA - Preferred Reporting Items for Systematic reviews and Meta-Analyses

SBS - Small Business Standards

SMEs – Small and Medium Enterprises

TX – Text

UE- European Union

US – United States

# 1. INTRODUCTION

## 1.1. BACKGROUND AND PROBLEM JUSTIFICATION

Over the years we have observed several changes in society mainly influenced by technology. Companies have never been more present in digital, which exponentially leads to the creation and sharing of data within companies, between partners and customers (i.e., stakeholders). With the new challenges brought by Covid-19, companies had to implement digital solutions faster than ever ('Horne & 'Joyce, 2021). Thus, it is understood that digital is extremely crucial for organizations in the course of their activity (Urbach et al., 2019). However, digitalization also means that companies are more exposed to new vulnerabilities, which forces companies to take effective security measures. Attacks on technological devices are disclosed in the news daily (Hiller & Russell, 2013). According to the ISO/IEC 27002 (2013), unauthorized accesses or incorrect practices affect companies, in a way that becomes more exposed to cyberspace. Cyberspace is less secure than it was 10 years ago, since there is currently a facility to access vital information on networked computers, and this leads to an increase in cyberattacks. According to the World Economic Forum's Global Risk 2021 report, cybersecurity failures is included among the highest's likelihood risks of the next ten years (Mclennan, 2021). This global growth of cyberattacks has led to several incidents such as exposing data from different users, at both organizations and governments ('Horne & 'Joyce, 2021). Cyberattacks and security breaches are no longer an exception (Arora et al., 2006). According to EY Global Information Security Survey 2020, a higher percentage of the firms (59%) mentioned that have faced an incident in the past 12 months related to cyber and privacy threats (Kris Lovejoy, 2020).

As stated in the IDC Portugal report, the pandemic has reinforced the security risk. The majority of organizations asked whether decision-makers noticed any change in the external risk environment given the current pandemic scenario, 74% of organizations answered yes, which increased, 25% answered that the level of risk remained constant and only 1% said that the risk decreased. Also, ask about the degree of confidence in the information security of their organization, given the evolution of the pandemic scenario, the answers are already more diverse: 11% of decision-makers are extremely confident, 33% are confident, 50% of organizations are somewhat confident, 5% are unconfident and only 1% of organizations say they are not confident. With the pandemic scenario, the environment on organizations has also changed, especially on cybersecurity. Many employees have started working remotely, so the risk of incorrect settings is higher, which creates a perfect environment for hackers to attack and be well succeeded.

It was also observed that most Portuguese companies plan to increase their cybersecurity expenses. The report indicates that 62% of managers will increase their cybersecurity expenses, 34% will maintain and only 4% of managers will decrease their expenses in these areas (Figueiró, 2021).

Companies can't be fully protected from cyberattacks. However, entities must have in mind a security strategy that makes it possible to identify, protect, detect and respond to potential cyberattacks. Thus, the National Institute of Standards and Technology (NIST) was developed a framework of security guidance for private companies in the US (Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018).

This framework consists of 5 core functions: identify (enable a better knowledge of the organization to manage cybersecurity risks to systems, assets, resources, people and data); protect (develop and implement the appropriate measures to mitigate the risks of cyberattacks); detect (develop and implement the appropriate activities to identify any event harmful to the organizations); respond (develop and implement appropriate activities to give the best response to cyberattacks); lastly, recover (develop and implement appropriate measures to maintain the proper functioning of the organization's services that have been harmed by a cyberattack).

Lately, we have verified some losses in organizations caused by cyberattacks, since they are not prepared for these invasions and do not know how to prevent themselves. Just one successful security breach, theft, error, hack or virus attack on a company can result in reputation and financial damage (Gordon et al., 2011). According to EY Global Information Security Survey, only 36% of the firms mentioned that cybersecurity is involved correct from the planning stage of new business plans (Kris Lovejoy, 2020). Cybersecurity is now one of the biggest challenges of companies and has become a matter of global relevance and importance (von Solms & van Niekerk, 2013). In addition to the existing risks from the external environment, insiders (employees) are a factor that may be taken into account for the company's security (Steele & Wargo, 2007). All individuals have heard about this word; however, their behaviour does not demonstrate the level of awareness needed to mitigate the risks of cyberspace (de Bruijn & Janssen, 2017). According to the Annex A of ISO 27001, exists 14 categories that select the right controls to grab the information security risks required by organizations (Phirke & Ghorpade-Aher, 2019b). The domains may be (1) Information security policies; (2) Organization of information security; (3) Human resource security; (4) Asset management; (5) Access controls; (6) Cryptography; (7) Physical and environmental security; (8) Operations security; (9) Communications security; (10) System acquisition, development and maintenance; (11) Supplier relationships; (12) Information security incident management; (13) Information security aspects of business continuity management; (14) Compliance.

The threats caused by cyberattacks that substantially affect a company's systems cannot be addressed completely by perimeter security solutions (Jones & Horowitz, 2012), also, many organizations have complex technological architectures, which leads to risks of cyberattacks ('Horne & 'Joyce, 2021). Therefore, it is up to organizations to take measures to be prepared for the issues of cyberspace. Thus, they need to understand their business environment and know where they are more vulnerable to take the adequate security strategy. "In today's hyperconnected world, companies need to consider multiple areas of cyber risk throughout their ecosystem" ('Horne & 'Joyce, 2021).

Using a security toolbox to help organizations from the risks of cyberspace could be a good solution to improve the security of businesses, and that may be considered to support the employees to mitigate the risks and reduce the impacts of cyberattacks. The different elements of a security toolbox will increase the probability of identifying and stopping a cyberattack. Awareness evolves the development of security architecture to provide knowledge about the functions of certain systems, how they communicate with each other and the requirements for a great performance of the systems. In this way, awareness allows applying the right plans to mitigate the risks of certain cyberspace threats (Jones & Horowitz, 2012).

The focus of the security toolbox will be the small and medium enterprise (SME). The SMEs are categorized according to the criteria defined by the European Commission: number of employees, annual turnover and annual balance sheet. Following article 2 of the Commission Recommendation, the class of SMEs is made up of enterprises that hire less than 250 people and which have an annual turnover not exceeding 50 million Euros, and/or an annual balance sheet total not exceeding 43 million Euros (European Commission, 2003).

## 1.2. STUDY RELEVANCE AND IMPORTANCE

Year after year, cybersecurity has been gaining attention and importance in the research community. The research community needs the right support tools to be effective in improving cybersecurity in society. So, new inputs for the research community can lead to a deeper knowledge of cybersecurity. The security toolbox may be seen as a vantage to the science because will help to develop the research related to improving the techniques and tools disposal to mitigate the high risks of cyberspace. The framework proposed reflects statements that can be explained by scientific theories and scientific research can improve cybersecurity practices.

In general, the different security solutions have relevant importance in society but let takes a look at the business environment. The increased concern by SMEs to protect their businesses from potential cyberattacks stimulates the need for managers to design new tools to support employees in the implementation of adequate measures to mitigate the risks of cyberspace.

The implementation of a security toolbox that helps SMEs to identify, protect, respond and recover from potential cyberattacks, may be relevant and can provide great results for different organizational environments to mitigate the risks of cyberspace. The capabilities of the framework can be integrated into different ways, so makes it possible for entities to stop attackers from manipulating a system, identify whether the system has been compromised, thus preventing the system from being damaged and isolating the different systems components that have been compromised for a better facility in restoring the system and allow managers to understand if the event occurred has been caused by a cyberattack or not.

SMEs have some struggles in the implementation of the necessary steps to avoid possible cyberattacks. The suggested framework would play an important role, to the users of the security Toolbox to get more know-how to protect the business environment from cyberspace. Facing the issues of cyberspace, as already mentioned in this research, a security toolbox may provide practical controls on how to protect the business from possible attacks. Getting awareness of the best control options for the higher protection of the business environment, would be good insights for future users since they will become less vulnerable to cyberattacks.

It is possible to identify some benefits for organizations through the use of the framework in the different phases of a cyberattack, which justify the relevance and importance of using it. Firstly, we can categorize the different phases of a cyberattack in the following way: (1) pre-attack phase; (2) attack phase; (3) post-attack phase. The toolbox will force attackers to adopt more sophisticated methods for their attack to be successful. Thus, it is perceived that the framework may be crucial in the pre-attack phase since it makes it difficult to manipulate the data of the systems. The several components of the framework together rise the like-hood of detecting and blocking a cyberattack (attack phase). Last but not least, the framework holds the data of events that have occurred, which allows a forensic analysis (post-phase). Therefore, it allows to the organizations take the appropriate actions to prevent another cyberattack.

## 1.3. STUDY OBJECTIVES

The goal of this paper is to design a security toolbox capable to identify, protect, detect and respond to potential cyberattacks.

To achieve this goal, the following intermediate objectives were defined:

- Study all relevant literature associated with cybersecurity to understand the current state of security solutions in the organizational environment;
- Design a security toolbox;
- Define a set of different applications for a security toolbox; and,
- Validation of the security toolbox.

It is expected that the results obtained will allow SMEs to protect themselves against the various risks associated with cybersecurity.

Thus, to ensure a good understanding and a more detailed analysis of the problem identified in the section 1.1, it will be carried out a theoretical study (chapter 3) associated with cybersecurity and its relationship with SMEs.

## 2. METHODOLOGY

The required output of this research is designing a security toolbox that helps SMEs to implement adequate measures to become more protected from cyberspace. For that, a Design Science Research (DSR) methodology will be the appropriate method to acquire the best quality data.

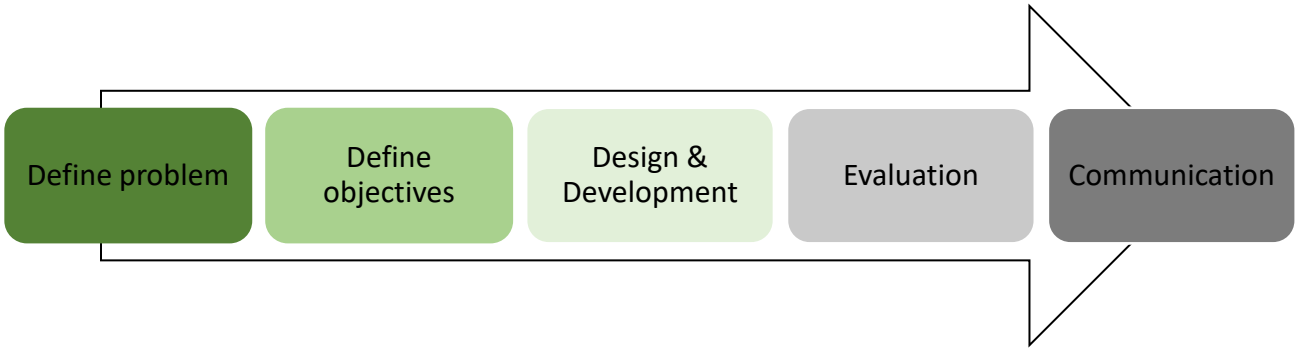
### 2.1. DESIGN SCIENCE RESEARCH

DSR approach seeks to increase the boundaries of human and organizational competencies by constructing new and innovative artifacts. In this paradigm, awareness and understanding of a problem domain and its solution are reached in the construction and application of the proposed artifact (A. R. Hevner et al., 2004) As stated by March and Smith, DSR consists of two activities: build and evaluate. Where the building is the process of designing an artifact for a certain problem and evaluating is the process of determining how well the artifact performs. The artifact performance is related to the environment in which operates. Thus, a full understanding of that environment may be essential for the success of the methodology (March & Smith, 1995). According to Hevner and Chatterjee, an artifact can be defined as an object created to solve a specific problem, proposed by natural objects (A. Hevner & Chatterjee, 2010).

Thus, it is perceived that the security toolbox can be considered an artifact since it is an object with a specific purpose, i.e., to solve the problem already mentioned. For that approach, we as a research community must provide well-defined and consistent definitions, ontologies, guidelines for the design and execution of the methodology mentioned (A. R. Hevner, 2007). So, for the development of the DSR, we will take into account two models that will help us to incorporate the practices and procedures necessary for the implementation of this research.

Firstly, it is important to considerer the design science research methodology (DSRM) proposed by Peffers for the construction of the DSR. Thus, 5 vital steps will be addressed in this research: (1) Define the problem; (2) Define objectives; (3) Design & Development; (4) Evaluation; (5) Communication (Peffers et al., 2007).

**Figure 1 - DSRM Adaptation** (Peffers et al., 2007)




I. Define problem

The definition of the research problem is a fundamental step to develop the artifact. Additionally, it is essential that the problem identified, and the solution proposed are unserstood and accepted by the interest parties (Peffers et al., 2007).

II. Define objectives

After the identification of a research problem, it is necessary to define objectives between, what is possible and what is feasible, to understand the necessary steps for the construction of the artifact (Peffers et al., 2007).

III. Design & Development

The next phase to follow, is the creation of the artifact. In this step, it is essential to carry out research through the state of art and the theoretical background, based on the research problem defined (Peffers et al., 2007).

It is argued by different authors that the knowledge of the state of the art (i.e., the current solutions available) is necessary and crucial to design the artifact. With this knowledge, the process of identifying utility gaps and overcoming current problems becomes easier (A. R. Hevner et al., 2004).

IV. Evaluation

In this phase, it is important to validate if the results obtained with the created artifact correspond to the defined objectives (A. R. Hevner et al., 2004).

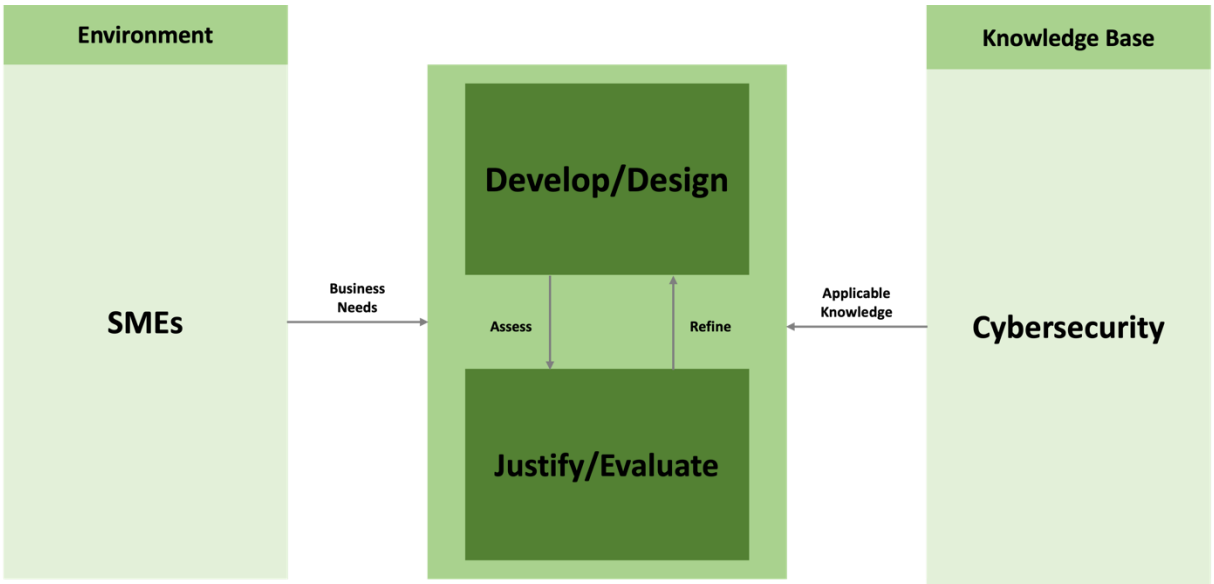
There is a wide variety of approaches to take in this step, but it is important to bear in mind that the selection of the assessment approach should be consistent with the proposed artifact (A. R. Hevner et al., 2004).

V. Communication

Lastly, it is important to communicate the identified research problem and its relevance to the public, together with the proposed artifact (Peffers et al., 2007). In this sense, it is crucial to share with the public the necessary details in order for them understand the proposed solutions and the usefulness of its application.

It is also important to consider the framework proposed by Hevner, to understand, execute and evaluate the research proposed combining behavioral-science and design-science paradigms. Thus, it is necessary to understand the business needs of SMEs and apply the knowledge in the area of cybersecurity to develop and build a security toolbox, to justify and evaluate the results of the artifact (A. R. Hevner et al., 2004).

**Figure 2 - IS Research Framework Adaptation** (A. R. Hevner et al., 2004)




## 2.2. RESEARCH STRATEGY

In the first step, a literature review will be executed to study all relevant literature associated with cybersecurity to understand the current state of security solutions in the organizational environment. Only with a clear understanding of the state of the art, it is possible to correctly define a problem in the SMEs environment.

In this sense, the literature review will be divided into different sections, namely:

- The main concepts of cybersecurity (that include the evolution of cybersecurity definition, the most common attack methods and the concept of computer security, information security and systems security);
- The different areas of security according with the ISO/IEC 27002:2013;
- Some tools & techniques that SMEs have available in the market (e.g., the NIST Framework and the training material proposed by the ENISA – EU Agency for cybersecurity);
- The challenges and opportunities that will help us to design an useful tool box for SMEs mitigate the risks of cyberspace; and,
- Lastly, a systematic literature review will be executed to understand the current state of security solutions in the organizational environment.

The systematic literature review process will allow the identification of gaps to design the security toolbox, according to the selected exclusion and inclusion criteria. Thus, the PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) Statement will be adopted, that resides of a 27 item checklist and flow diagram divided in 4 different phases (Moher et al., 2009). With this in mind, we believe that PRISMA Statement will be useful to improve the quality of the report. In the process of systematic literature review, articles published before 2015 will be excluded, to obtain the most up-to-date information possible. Additionally, the articles will be selected using the ESBCO database. Furthermore, only articles written in English will be considered because will facilitate our interpretation.

Moreover, it should be stressed that only articles in the SMEs environment that contribute with techniques and methods to improve cybersecurity practices and behaviors will be considered. Finally, to help us in the selection of the appropriate articles, the following keywords will be considered: “Security Toolbox AND SMEs”, “Cybersecurity Awareness AND SMEs”, “Cybersecurity Education and SMEs” and “Security Techniques AND SMEs”.

With the literature review it is expected that we will have the necessary and adequate information, given the strategy adopted, to design the security toolbox.

Afterwards, the main goal is understanding how well the security toolbox supports a solution to the problem identified (Peffers et al., 2007). The evaluation phase will be performed by focus group meetings with the purpose to discuss a particular topic. That approach may be useful to generate valuable information since promotes sharing of participants’ viewpoints and experiences (Gill et al., 2008). In the end, an analysis of qualitative data obtained in the focus groups meetings will be made.

Finally, a performance to a technical and non-technical audience will be presented in the communication step since it is vital to understand how operational the artifact is (A. R. Hevner et al., 2004).

# 3. BACKGROUND RESEARCH

Throughout this section, the theoretical bases necessary for the construction of the security toolbox will be presented.

In this sense, the literature review aims to understand the main theoretical concepts associated with cybersecurity and understand the needs of SMEs according to the cybersecurity risks they face. Thus, the literature review was divided into two parts.

In the first part, the concepts and different areas associated with cybersecurity were investigated. Additionally, existing techniques and tools on the market that help organizations mitigate the risks associated with cybersecurity were researched. Lastly, the challenges and opportunities associated with cybersecurity were identified, which will be an important input to design the security toolbox.

In the second part, and adding to the preliminary research presented in the section 3.1, a Systematic Literature Review was carried out following the PRISMA methodology.

## 3.1. CYBERSECURITY

### 3.1.1. Concepts

Before cybersecurity was a well-known term, computer security studies were already conducted. Computer security is dismantled in two subthemes, i.e., information security and systems security, having these terms launched the cybersecurity (Christen et al., 2020) The authors reported that “information security is concerned with the protection of (potentially processed by computers) and any information derived from its interpretation” and “systems security aim to ensure that (computer) systems operate as designed, i.e., attackers cannot tamper with them”.

In 1972, Anderson proposed the CIA (Confidentiality, Integrity and Availability) triad (Anderson, 1972), that has been used as the basis for all cybersecurity. In the course of time, new approaches were developed because in the CIA triad the risks associated with cybersecurity were not fully understood (Ham, 2021).

Consequently, other proposals were developed, for example, the NIST cybersecurity Framework (Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018). This framework consists of 5 core functions: identify (enable a better knowledge of the organization to manage cybersecurity risks to systems, assets, resources, people and data); protect (develop and implement the appropriate measures to mitigate the risks of cyberattacks); detect (develop and implement the appropriate activities to identify any event harmful to the organizations); respond (develop and implement appropriate activities to give the best response to cyberattacks); lastly, recover (develop and implement appropriate measures to maintain the proper functioning of the organization's services that have been harmed by a cyberattack).

Over the years, the cybersecurity has gained popularity, being seen as a subject with a particular perspective. Thus, it is understood that there are several definitions for this theme, and it is also variable conforming with the context (Craigen et al., 2014).

Through the literature review, it was possible to obtain some definitions of cybersecurity:

**Table 1 - Definitions of cybersecurity**

| Author: | Definition: |
|---|---|
| (Kemmerer, 2003) | *"Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders"* |
| (ITU, 2009) | *"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets"* |
| (Chang, 2012) | *"Cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines"* |
| (Canongia & Mandarino, 2014) | *"The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting in cyberspace, its information, assets, and critical infrastructure"* |

| Author: | Definition: |
|---|---|
| (Schatz et al., 2017) | *"The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space"* |
| (Wiederhold, 2021) | *"Cybersecurity is the measures we take to protect our technology, and thus our information, against theft and misuse. While cybersecurity today is about so much more than putting a sticky note over your laptop's camera when not in use, who has the time or energy to put into keeping personal and corporate information private?"* |

There are several cybersecurity risks that are present in the organizational environment and should be considered, namely (Zúquete, 2021):

- Intrusion: this risk is caused by a set of actions aimed at compromising the integrity, confidentiality, or availability of a particular resource/asset. Basically, intrusion results from one or more attacks on an organization's system that manages a certain resource/asset. This type of attacks may or may not compromise the information stored in the affected system. According to the author, this risk is considered difficult to assess as there is no need to involve data however it grants access to something that would be denied to the intruder.
- Access to confidential/restricted information: All unauthorized access to information is considered by the author a risk that should be considered.
- Loss of theft of information: According to the author, this risk encompasses situations in which information is lost or stolen by unauthorized persons.
- Personification: This risk identified by the author occurs when an intruder manages to sabotage an authentication system in two ways, i.e., by impersonating an authorized person or when causing changes to the behavior of certain applications.

In addition to what has already been mentioned, it is necessary to understand the difference of the different types of cyberattacks since different types of solutions will be needed to mitigate these issues. The most common attack methods are:

**Table 2 - The most common attack methods adaptation** (Adeyinka, 2008)

| Type of attack | Definition: |
|---|---|
| Viruses | Viruses are self-replicating programs that infect and spread through files. They are usually activated when a file is opened because the viruses are attached to a file. The viruses have different properties, i.e., multi-partite, stealth, encrypted, polymorphic or macro virus. The first property, multi-partite, means that viruses are hybrid because they can contaminate files and systems and/or boot-records. The second property, stealth, means the virus try to hide its presence from the users, attaching itself to files that normally are not seen. Additionally, the viruses can use encryption to hide their payload. Viruses with this property are hard to identify and analyze. Other propriety of viruses is called polymorphic, that means viruses can resist a longer time without being extinguished because their signature is changed over time. Finally, the macro virus, that produce macros for popular programs that are malicious, e.g., this property can insert/delete data from a excel sheet. |
| Phishing | This type of attack passes through third parties trying to obtain confidential information to gain a financial return. They are usually groups of individuals who try to trick people to obtain confidential data, such as credit card numbers, usually via email. |
| Trojans | Trojans are attached to programs that at first glance are trustworthy but actually contain malicious content. Subsequently, they have the ability to remotely access an individual's device or even a virus. |

| Type of attack | Definition: |
|---|---|
| Hacking | Currently, there are criminal with strong qualifications in the use of computers, which are called hackers. These individuals analyze vulnerabilities in a device or a system and then access or attack them. |
| Email bombing and spamming | The email bombing is an email attack where identical messages are constantly sent to a specific email address. Email spamming is a variant of bombing, but in this case, email is sent to thousands of different email addresses. This type of attack could be combined with email spoofing, thus making it more difficult to understand who is the real email sender. |
| Denial of Service (DoS) | This attack happens when a system getting the demands gets busy, trying to set up a return communications way with the initiator (which may or may not be employing a substantial IP address). The targeted host collects a TCP SYN and returns a SYN ACK. It at that point remains in a hold up state, foreseeing the completion of the TCP handshake that never happens. Each hold up state uses system resources until inevitably, they cannot react to another legitimate request. |
| IP Spoofing Attacks | Spoofing allows attackers to forge them identify using a trusted computer and thereby gain unauthorized access to other computers. A malicious attacker could gain access by spoofing the source IP address of packets sent to the firewall. Thus, the firewall can allow the access to the address used, thinking that it a trusted host identity. |

| Type of attack | Definition: |
|---|---|
| Worms | It is a program that replicated itself on the network, but unlike viruses, it does not need an affected file to be propagated. It is possible to identify two different types of worms, mailing worms (i.e., it is sent via email. The email sent to the recipient contains a virus or a trojan) and network-aware worms (i.e., it is a worm that attacks on the internet. Firstly, the compromised host targets a host. After that, the compromised host try to gain access to the target host by exploitation. When the worm gets access, it can infect it, for example, with trojans.) |
| System and Boot Record Infectors | This type of attack infects system areas of computer (e.g., MBR on hard disks and the DOS boot record on floppy disks). When this virus installs itself in the boot records, it manages to run whenever a computer is booted up. |
| Eavesdropping | This attack happens when an unauthorized party intercepts or gets access to communications. It is possible to identify two types of eavesdropping, the passive (i.e., an unauthorized person that can listen messages from the network without anyone detecting them) and the active (i.e., it is a person who, in addition to being able to hear network communications, can interfere with the communications to distort or create false messages). |

Thus, given the types of cyberattacks mentioned, it becomes crucial for organizations to create solutions to mitigate these dangers of the digital world. So, it is necessary to consider the different areas of security, which will be described in the section 3.1.2.

Additionally, it is necessary to consider the definition of SMEs, since the objective of the research will be designing a security toolbox for SMEs. As mentioned in the section 1.1, SMEs are categorized according to the criteria defined by the European Commission: number of employees, annual turnover, and annual balance sheet.

Following article 2 of the Commission Recommendation, the class of SMEs is made up of enterprises that hire less than 250 people and which have an annual turnover not exceeding 50 million Euros, and/or an annual balance sheet total not exceeding 43 million Euros (European Commission, 2003).

### 3.1.2. Security Domains

Currently, security in organizations is a crucial point for their success. The standards ISO/IEC 27000, 27001 and 27002 are international standards for information security (Disterer, 2013). The ISO/IEC 27001 help companies to adopt better security measures (Phirke & Ghorpade-Aher, 2019b). As stated by the authors, the ISO/IEC 27001 aims to perform an Information Security Management System (ISMS) in a company. Basically, the ISMS applies different tools and methodologies necessary to ensure confidentiality, integrity, and the availability of the information systems (Phirke & Ghorpade-Aher, 2019a).

The ISO/IEC 27002:2013 gives different guidelines and information security management practices to the organizations consider. This standard is divided in 14 security control domains collectively containing a total of 35 main security categories and 114 controls (2013). Which domain define security controls that contains one or more main security categories. As mentioned in the ISO/IEC 27002:2013 the organizations should identify applicable controls and understand how important these are and their application to certain business processes. The main security control categories contain the following:

a) A control objective with what is expected to be achieved; and,
b) Controls that can be adopted to achieve the main control objective.

Which control mentioned in the ISO/IES 27002:2013 are structure as follows: (i) control, that explains the control statement to achieve the control objective; (ii) implementation guidance, that gives detailed information to support the adoption of control measures considering the control objective; (iii) other information, that contributes with information that is usefull to be considered (e.g., legal considerations).

According with the ISO/IEC 27002:2013, the 14 security control domains may be:

Information security policies

This domain contains the management direction for information security category that focus on providing guidance and support for information security according to the requirements of the organization and its environment.

Organization of information security

This domain holds the internal organization category that aims to implement a management framework to introduce and control the implementation and operation of information the organization. Furthermore, this domain contains the mobile devices and teleworking category that provides polices to guarantee the security of the use of mobile devices and teleworking.

Human resource security

This domain covers the prior to employment category that ensure that employees and other people that are related with the organization are aware of their responsibilities and can perform the assigned functions. Additionally, includes the during employment category that guarantee the employees and other people related with the organization are alert and accomplish their information security information security responsibilities. Lastly, contains the termination and change of employment category that aims to safeguard the organization's interests.

Asset management

This domain holds the responsibility for assets category that aims to identify the organizational assets and set proper protection responsibilities. Moreover, includes the information classification category which aims to guarantee that the information has the adequate protection according to their importance for the organization. Last but not least, this domain covers the media handling category with the objective of mitigate the expose, alteration or destruction of information stored on media.

Access control

This domain contains the business requirements of access control category that provides policies to limit the access to information and information facilities. Also, this domain holds the user access management category that is based on helping organizations that only authorized users have access to the systems and services. Finally, this domain covers the system and application access control category that specifies policies to prevent unapproved access to systems and applications.

Cryptography

This domain includes the cryptographic controls category to enable organizations to take appropriate and effective cryptographic measures to protect the confidentiality, authenticity and/or integrity of information.

Physical and environmental security

This domain contains the secure areas category that provides measures to allow only authorized persons to have access to the physical areas of the organization and to prevent damages and interferences in the company's information and information processing facilities. Furthermore, the domain covers the equipment category with the objective of prevent and mitigate the risk of loss, damage, theft or compromise of assets and interruption of the business processes.

Operations security

This domain contains the operational procedures and responsibilities category which aims to ensure that information processing facilities are safe and properly configured. Moreover, includes the protection from malware category to enable protection from malwares to the information and information processing facilities. Furthermore, this domain holds the backup category that is based on helping organizations mitigate the risks of data loss. Also, covers the logging and monitoring category which aims to register events and create evidence. Additionally, contains the control of operational software category with the objective of provide controls to ensure the integrity of operational systems. In addition, this domain contains the technical vulnerability management domain to helps organizations prevent themselves from being invaded through technical vulnerabilities. Last but not least, covers the information systems audit considerations category that helps entities to mitigate the impacts of audit actions on operational systems.

Communications security

This domain holds the network security management category that provides controls to protect information in networks and its supporting information processing facilities. Also, contains the information transfer category which aims the security of change of information between an organization and an external entity.

System acquisition, development, and maintenance

This domain includes the security requirements of information systems category that provides controls to ensure that information security is included throughout the life cycle of the organization's information systems. This category also includes the needs for information systems which provide services over public networks. Furthermore, this domain contains the security in development and support processes category which aims to guarantee that information is defined and implement within the development life cycle of the organization's information systems. Finally, covers the test data category that provides controls to help organizations in the protection of data that is used for testing.

Supplier relationships

This domain holds the information security in supplier relationships that gives guidelines of how organization can protect their assets that is accessible by suppliers. Additionally, contains the supplier service delivery management category which helps organizations maintain the level of information security and ensure that service delivery complies as agreed with suppliers.

Information security incident management

This domain covers the management of information security incidents and improvements category which has the objective of ensure that the management of information security incidents is effective and consistent, which includes the communication of events and weaknesses.

Information security aspects of business continuity management

This domain includes the information security continuity category to ensure that information security is included in the organization's continuity management systems. Finally, this domain holds the redundancies category that helps organizations to guarantee the constant availability of information processing facilities.

Compliance

This domain contains the compliance with legal and contractual requirements category to help organizations keep away from breaches of legal or contractual obligations related to information security or other security requirements. Last but not least, includes the information security reviews category to ensure that information security is in compliance with the organization's policies and procedures.

In 2013, the Small Business Standards (SBS) – an European association that represents SMEs – established an SME guide for the implementation of ISO/IEC 27011, with the purpose of facilitating these companies to implement the different levels of information security in accordance with the standard (Guasconi et al., 2013)

### 3.1.3. Tools & techniques

Nowadays, it is essential for organizations to protect from the various attacks already mentioned. Cyber-attacks over the years have increased, being these more complex and sophisticated (Hruza et al., n.d.). It is necessary for companies to detect, analyze and defend, in real time, from cyberspace threats, which is not possible without the resource of threat intelligence, big data and machine learning techniques (Cabaj et al., 2018). Thus, this chapter will describe several tools, models and techniques that help organizations to mitigate the various risks of cyberspace.

NIST Cybersecurity Framework

In February 2014, the National Institute of Standards and Technology (NIST) have proposed a cybersecurity framework with the objective of mitigate cybersecurity risks (Stine et al., 2014). The framework includes security measures and controls to help organizations identify, assess, and manage cyberspace-related risks, thereby protecting entities from aspects related to confidentiality and individual privacy. The framework proposed by NIST was divided into three components, namely:

1) Framework Core;
2) Framework Profile; and,
3) Framework Implementation Tiers.

The **Framework Core** presents standards, guidelines, and practices available to various industries, to allow the communication of cybersecurity activities through the entire organization. The first component under analysis is divided into five functions – Identify, Protect, Detect, Respond and Recover. These functions, as a whole, provides to the organizations a strong vision for manage cybersecurity risks. For each function, categories and subcategories are identified and combined with reference examples such as existing standards, guidelines, and practices.

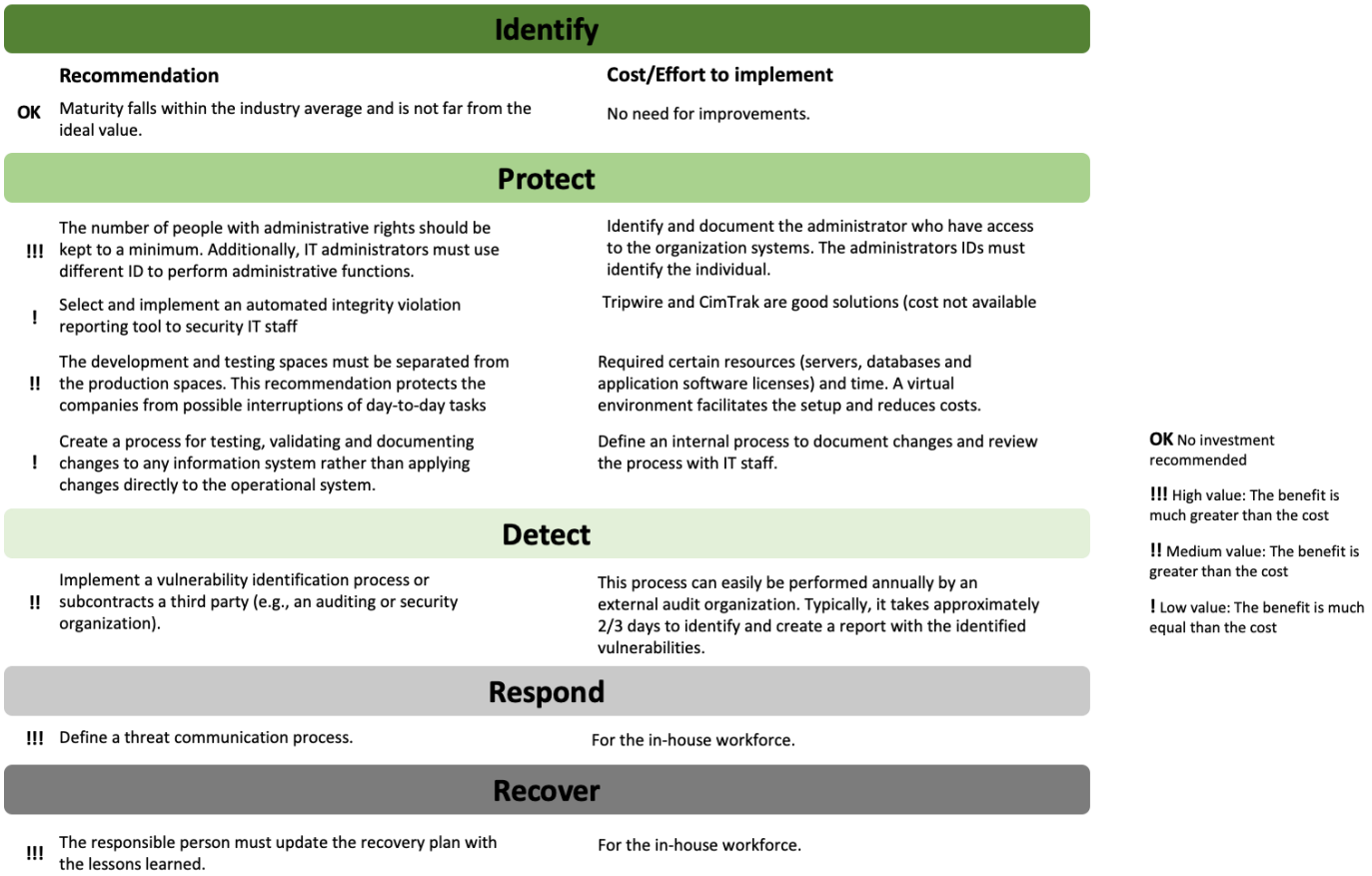
The **Framework Profile** presents the results obtained according to the needs of the organization selected in the Framework Core (categories and subcategories). The profile to be adopted will be characterized based on the alignment of standards, guidelines, and practices, and that will be useful to identify opportunities for improvement in cybersecurity. For the development of the company profile, it is necessary to consider the categories and subcategories obtained, to carry out a risk and importance assessment for it. This method become important since it allows companies to self-evaluate and communicate results internally or externally.

Last but not least, the **Framework Implementation Tiers** presents context of how companies look at cybersecurity risks and what processes they have to manage those risks. In the tier selection process, it is critical that the organization consider the current risk management practices, its surroundings with regards to threats, laws and regulatory requirements, the company's objectives, and its mission. Basically, the selected tiers describe the degree to which the companies' cybersecurity risk management practices represent the characteristics defined in the framework. These tiers are characterized according to a variable range from 1 (Partial) to 4 (Adaptable). To summarize, organizations can use the Framework proposed by NIST as a key tool for the process of identifying, assessing, and managing cybersecurity risks. This framework was not created to replace existing processes, but to add to organizations a tool that allows to determine gaps in cyber-risk management approaches and create opportunities for improvement.

The NIST Cybersecurity Framework has some limitations. As already mentioned, it is an important tool to apply principles and practices to mitigate cybersecurity risks, nonetheless it is complex which makes it application in organizations difficult. Additionally, despite allowing the assessment of the defined standards by the organizations, there no exist classifications considered acceptable for these standards. Moreover, in the absence of comparative data, it becomes impossible for organizations to quantify the effectiveness of defined safety policies and practices (Mijnhardt et al., 2016). Lastly, the NIST Cybersecurity Framework does not present good practices or recommendations to improve security in organizations, which means that organizations are obliged to define their improvement objectives according to their surroundings (Abraham et al., 2019).

In this sense, Michael Benz and Dave Chatterjee proposed an SME Cybersecurity Evaluation Tool (CEF) based on 35 standards defined by the NIST Cybersecurity Framework, which are the most relevant given the risks that SMEs need to face (Benz & Chatterjee, 2020). The choice of only 35 standards and not the 96 defined by NIST is due to the fact that SMEs have limited resources. Thus, SMEs can apply efforts where there is a greater impact, according to the authors. Furthermore, the authors proposed some recommendations to improve cybersecurity maturity in SMEs, according to the figure below.

**Figure 3 – Recommendations to improve cybersecurity maturity adaptation (Benz & Chatterjee, 2020)**




As reported by Michael Benz and Dave Chatterjee, IT leaders to benefit from the proposed framework, should carry out an assessment of the identified risks and suggested recommendations, with the objective of create a plan to prioritize and implement the most appropriate practices.

Training material for SMEs

The ENISA - EU Agency for cybersecurity - have been created some training materials for SMEs to encourage employees to get more awareness about crucial and fundamental security issues. These training materials include email security, malicious software, identity theft prevention, use of the internet at home, security while travelling and last but not least security when working remotely (ENISA, 2020).

Basically, this training material provides insights to employees get more awareness about information security and help them to respond correctly to threats. The training material are divided in the following way:

**Figure 4 - The different training materials available for SMEs** (ENISA, 2020)

| Training material | What is included? |
|---|---|
| Email security | This training material is divided in two sections, 1) why email security is important (that will help employees realize their importance) and 2) how to use e-mail securely (that will provide some techniques and tips to employees to use the email correctly without compromising the company). |
| Malicious software | This training material is divided in two sections, 1) what is malicious software, how malicious software can affect you and types of malicious software (that will help employees get awareness about the risks related with malicious software) and 2) how to protect yourself and resources (that will provide some techniques and tips to employees to protect themselves from malicious software). |
| Preventing identity theft | This training material is divided in three sections, 1) what is identify theft and how does it happen (that will helps employees realize their importance and get awareness about the risks and the effects of identity theft), 2) how can you protect yourself (that will provide some techniques and tips to employees protect themselves) and 3) resources (that gives more information related with the topic). |

| Training material | What is included? |
|---|---|
| Online security at home | The covid 19 pandemic brought a new paradigm to the most employees, the teleworking. Thus, the risks may be higher, so it is essential to make employees aware. This training material is divided in two sections, 1) why security is important (that will help employees realize the importance of security when the internet is used at home) and 2) how to protect yourself and your family (that will provide some techniques and tips to employees protect themselves and their families) |
| Security when working remotely | This training material will complement the previous one and is divided in two sections: 1) why security is important while working remotely (that will help employees get awareness about the risks related with working remotely) 2) how to be secure while working remotely (that will provide some techniques and tips to employees protect themselves in teleworking). |
| Security while travelling | Such as working remotely from home, business travel can increase the risks associated with security. This training material is divided in three sections, 1) why security is important while travelling (that will help employees get awareness about the risks related with business travel), 2) what to do before you leave (that will provide some techniques and tips to employees prepare safely the business travel) and 3) what to do while you are there (that will provide some techniques and tips to employees protect themselves and the company). |

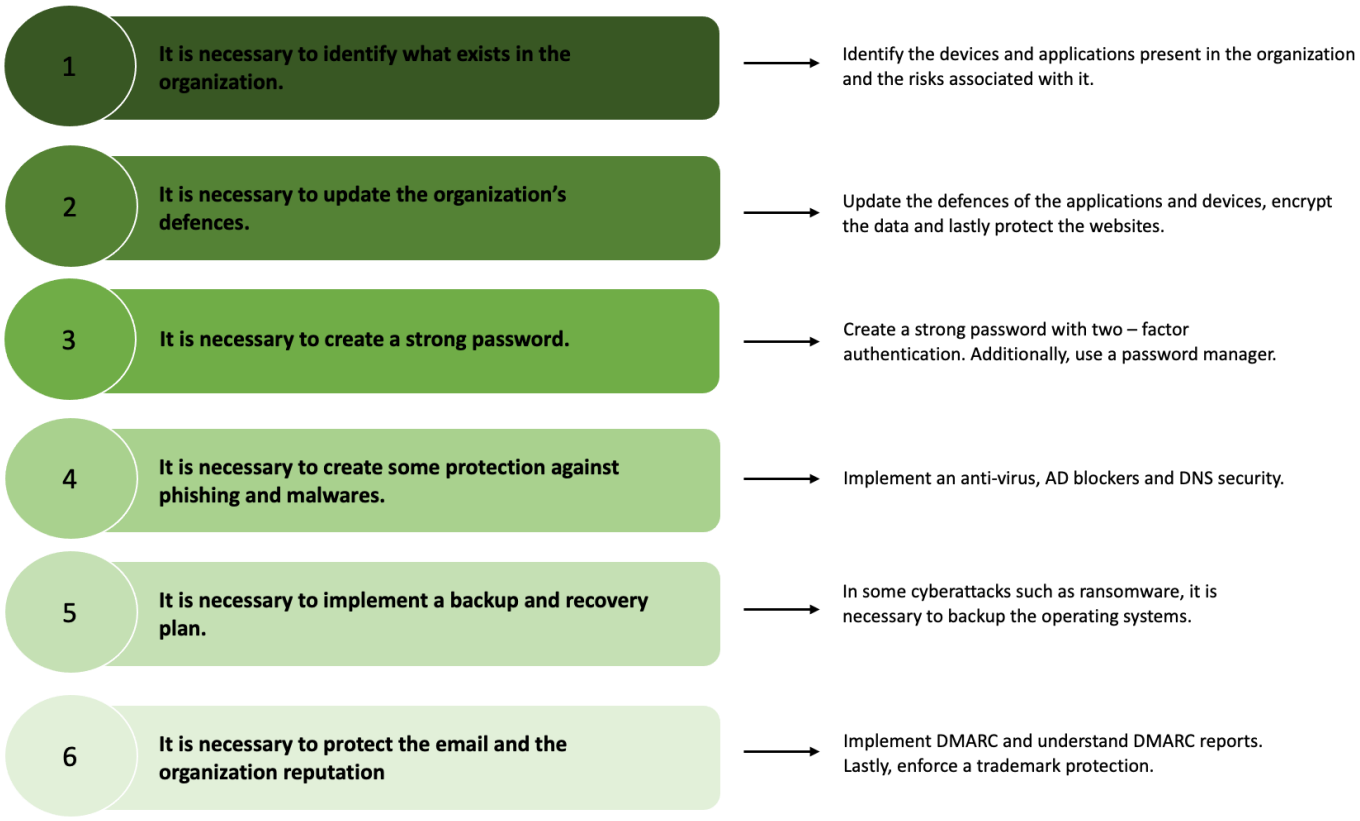
Global Cyber Alliance Toolbox

The Global Cyber Alliance develops several tools with the objective of mitigating the risks of cyberspace. These tools are organized to facilitate organizations to implement various security control measures associated with cybersecurity.

One of the tools available is the GCA Cybersecurity Toolkit for Small Business that was created to help SMEs but can be used by any type of organization. The mentioned toolbox is divided in 6 steps with certain necessary actions. It should be noted that the tool developed by the Global Cyber Alliance was designed for organizations with poor IT knowledge, few resources, and low budgets.

The figure below shows the steps and actions to be taken to improve security in SMEs.

**Figure 5 - GCA Cybersecurity Toollkit for Small Bussiness – Adaptation** (Global Cyber Alliance, 2019)



Network Visualization Systems

Today, organizations have some tools that provides information in real-time such as the attack source, attack type, attack destination, attacker's IP address and attacker's geographical location. This type of tool is called network visualization systems, which provides a visual map of cyber-attacks across the world.

It is possible to identify different solutions of network visualization systems, namely HoneyMap, Norse Map, Digital Attack Map, Kaspersky Cyberthreat Real-Time Map, FireEye Cyber Threat Map, Threat Cloud, Trend Micro, Akamai, Malwaretech Live Map and Fortinet Threat Map (Baykara et al., 2018).

Computer & Network Simulations

Another technique that can be used are computer and network simulations, which basically allow to simulate real attacks situations which allows employees of companies to be better prepared for the risks of cyber space. This type of simulations allows to realize if employees are prepared to comply with the company's policies without real consequences. An example, it might be a blacklist or whitelist assumption of certain websites that can be examined in the context of realistic models of user behavior (Veksler et al., 2018).

The authors mentioned several pure simulation models already studied, such as ns-3 (Riley & Henderson, 2010), Optnet (Xinjie Chang, 1999) and others. However, they argued that ns-3 could be the best choice because it is an open source, so the users can benefit from a from a large community backing the model. Although pure simulation does not overhead usage time, it does not have the ability to model actual payloads and timelines that are present in a normal network, and sometimes these assumptions may not reflect real-world traffic. Another downside of pure simulation is the fact that it does not give an insight of software behavior and only network traffic is modeled. (Veksler et al., 2018). Thus, the authors identified another approach, Hybrid Network Emulation, where software and network are modeled. This approach uses machine virtualization techniques such as QEMU-KVM (Habib, 2008) or XEN (Barham et al., 2003).

Free Cybersecurity Tools

According with Josh Johnson, businesses have some free cybersecurity tools available that can be used for every type and size of organization. The risks from cyberspace are increasing and some security tools can be very expensive (Johnson, 2021). Thus, the following list enumerate some free solutions available in the market that organizations can use

**Table 3 - Free Cybersecurity Tools Adaptation** (Johnson, 2021)

| Tool | Definition |
|---|---|
| Aircrak-ng | This solution includes a few tools to assess WIFI network security, that focus on different areas such as monitoring, attacking, testing, and cracking. |
| Burp Suite | A platform that helps in debugging and security testing web app security. |
| Gophish | This solution is an open-source platform that provides a few features that helps users to simulate and monitor elaborate phishing campaigns. |
| Have I Been Pwned | This is a website that allows users to understand if any personal information has been revealed through a data breach. |
| Kali Linux | Basically, this tool is an operating system for pen testing, security auditing and digital forensics. Includes pre-installed programs such as Arcracl-ng and Metasploit. |
| Metasploit Framework | It is an open-source platform that allows users to probe networks and applications to understand if there are some vulnerabilities and weaknesses. |
| Nmap | This tool provides some features that allow users to find network nodes and scan systems for weakness. |
| Nikto | This solution is helpful tool for uncovering weaknesses in web apps, services, and web servers. This tool also provides a feature to detect an intrusion in the systems. |
| OpenVAS | It is a vulnerability scanner with the advantage of being customizable, which makes it more flexible for the different needs of the companies. |

| Tool | Definition |
|---|---|
| OSSEC | A popular tool for evasion detection and prevention. One of its best features is that it can analyze logs, allowing users to compare log events from different sources. |
| Password managers | There are a different free solutions to manage the passwords such as the KeePass, Psono and Bitwarde. These tools have an important role because permits to safely store all passwords together in a system. |
| PfSense | It is an open-source firewall that can be configured to help users to detect and prevent evasions, traffic shaping and other features. |
| P0f | It is a tool that allows organizations to identify fingerprints and other vital information without interfering with the network. For this reason, despite being used by ethical hackers, it is also widely used by cybercriminals. |
| REMnux | This solution has some features that help users with reverse engineering and malware analysis. |
| Security Onion | It is an open source with certain features that allow users to monitor networks through packet capture, intrusion detection systems, log indexing, search, and data visualization. |
| Snort | This solution is an open-source platform with the ability to analyze and record network traffic in real time, which makes it important for the detection and prevention of unauthorized evasion. |
| Wireshark | It is a tool with some features that allow organizations to identify, locate and examine network packets to understand if there are vulnerabilities that lead to security flaws |

### 3.1.4. Challenges & opportunities

According to the SME Annual Report 2020/2021 carried out by the European Commission, SMEs represent the vast majority in Europe (around 99.80%) and it is estimated that produces 53.00% of added value. In this sense, the concern for SMEs in the areas of cybersecurity has been growing. With the Covid-19 pandemic, SMEs were forced to accelerate their digital transformation process, which according to the report created several challenges for them, namely: lack of mindfulness and availability of the technology and tools need to implement the digital transformation; lack of capacity in terms of time and cash; and lack of aptitude to combine a digital strategy with a particular business model (Muller et al., 2021). Thus, due to the low level of protection, ability to react and recover from cyberattacks, SMEs require special attention.

As reported by the Ponemone Institute in 2018, SMEs must deal with different challenges related with cybersecurity (Ponemon Institute LLC, 2018). These challenges are derived from the lack of **resources** (i.e., with the constraints on their resources, compared to large companies, SMEs are unable to make the necessary investments to implement adequate cybersecurity strategies), **expertise** (i.e., to implement cybersecurity strategies, knowledge in the area is required. However, SMEs have revealed a lack of wisdom regarding security measures), **responsibility** (i.e., responsibilities related to cybersecurity are not well defined in SMEs, so there is weak leadership capacity in cybersecurity related functions) and **technology** (i.e., most SMEs subcontract IT services providers externally which leads to increased risks as cybersecurity strategies are not defined internally).

Additionally, according to a survey made by Emma Osborn to 33 persons from SMEs, it was possible to draw certain conclusions (Osborn, 2014). First, the questionnaire was sent by email where employees would have access to the question via a link. A large percentage of respondents demonstrated that cybersecurity is something important to consider, however only a small percentage took the necessary steps by opening an external link to access the questionnaire. Another important conclusion was the fact that only half of the respondents mentioned that there is an IT team in their companies. Another factor to be considered, concerns to the support of incentives given to SMEs. Although there is support for this category of companies, the incentives are low developed and are focused on large companies.

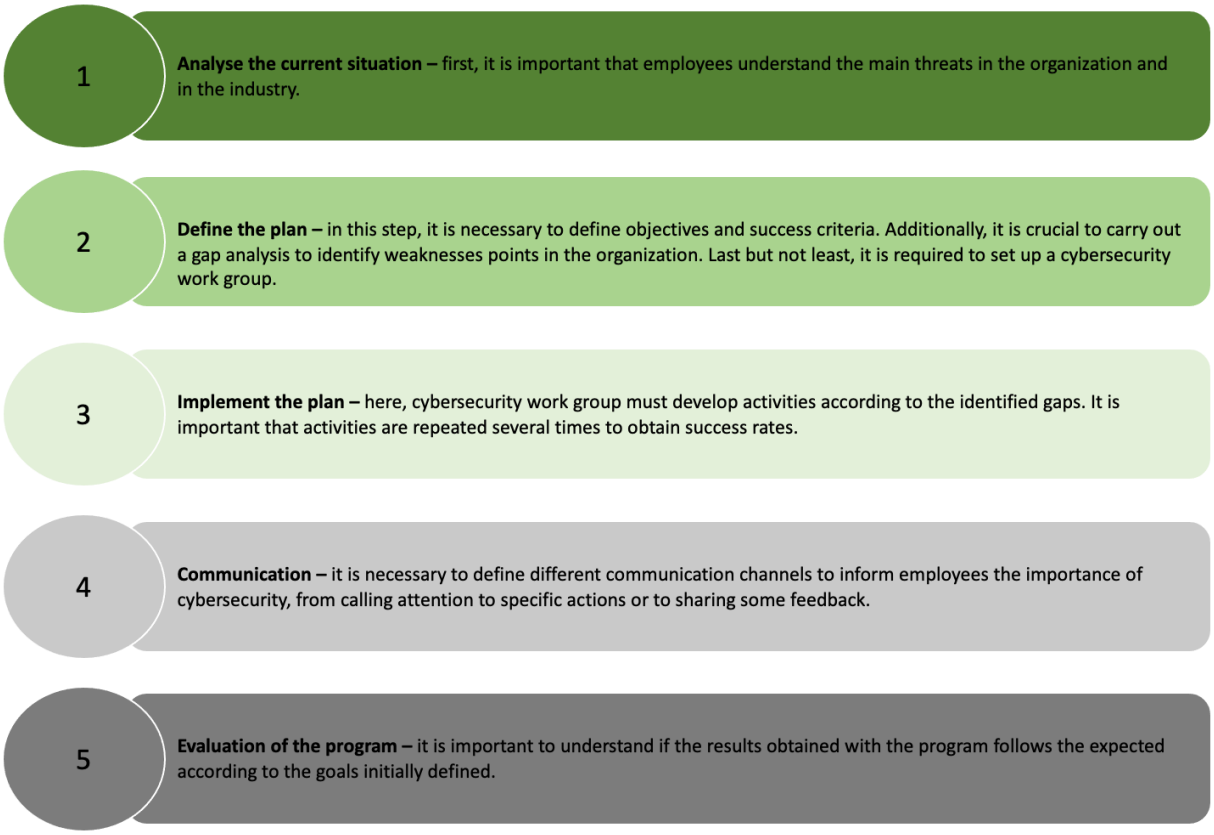
In the questionnaire, respondents were also asked what the greatest difficulties in cybersecurity were, where the answers were mostly lack of resources or knowledge.

Therefore, one of the key factors to improve the level of cybersecurity in SMEs is to raise awareness (Ponsard & Grandclaudon, 2020). The concept of cybersecurity awareness can be defined as the degree to which employees of a given organization understand the importance of IT security, the appropriate security standards for the organizations and their individual responsibilities for maintaining security in the organization (Information Security Forum, 2002).

In this context, and as already mentioned, SMEs in recent years have struggled to protect themselves from the risks of cyberspace due the lack of awareness, expertise, and resources (Paulsen, 2016). Nevertheless, several proposals have been coming up, with the aim of assisting SMEs to gain greater awareness, education, and training in cybersecurity. These new proposals have been come from academic research, industry governments, Federal Trade Commission and EU (Bada & Nurse, 2019).

As reported by Ashik, to implement awareness in organizations, it is necessary to follow some strategic key steps:

**Figure 6 - Steps for developing a cybersecurity culture program – adaptation** (Ashik, 2019)



Furthermore, Ponsard and Grandclaudon, stated that SMEs can raise cybersecurity awareness through general information available in different portals at different levels: European, national, or local security coalitions (Ponsard & Grandclaudon, 2020). For example, in Europe, the month of October was defined by the ENISA as the month of cybersecurity, where it is possible to check several tips or some activities to individuals check cybersecurity skills (ENISA, 2021). The authors also reported that posters can have positive and effective effects to implement cybersecurity awareness in SMEs because they are easy to produce and set in different communication channels. The ENISA, for example, have a several of posters with important security rules that SMEs can use to raise the cybersecurity culture (ENISA, 2019).

Moreover, Ponsard and Grandclaudon affirmed that guides allow SMEs to gain several insights into basic and advances cybersecurity measures. These guides depend on specific risks however generic checklists are available in the market, that can be easily used by SMEs. For example, was developed, by CIS – Center for Internet Security - 20 security controls and a guide to help SMEs implement these security controls (CIS, 2017).

In addition to the aforementioned, Ponsard and Grandclaudon also mentioned that personae could be a good technique to raise awareness. This method involves creating fictional characters with certain characteristics and behaviors. It should be noted that it can be an important technique to create awareness among employees, as it becomes possible to associate threats with risky behaviors of fictional characters (Ki-Aries & Faily, 2017). Moreover, this technique could be used to designing training or to communicate the importance of cybersecurity. For example, an employee may associate their behavior with a fictional character and thus realize that something needs to be changed to avoid certain risks associated with cybersecurity (Ponsard & Grandclaudon, 2020).

Learning through games can also be an effective technique, according to the authors. Gamification can be defined as a form of systems in which different players are engaged in a virtual environment with a specific goal and certain rules, involving the players to act to solve a problem (Kapp, 2012). Another author, Kate O'Flaherty, mentioned that gamification can be useful to raise awareness among employees as it makes it easier to understand the threats associated with cybersecurity (O'Flaherty, 2019). An accessible way to do it is through quizzes with the aim of helping employees deal with real situations and risks associated with cybersecurity. The authors argue that there are key factors for their success, namely: 1) the quiz organizers should do not know who is responsible for a given answer; 2) must be done in a group; and 3) must be visually attractive (Ponsard & Grandclaudon, 2020).

Another technique that the authors mentioned is the self-assessment. This technique, unlike quizzes, allows a deeper and a more structured evaluation. Regarding cybersecurity associated with SMEs, it is possible to identify initiatives created by Europe of different types of self-assessment (Ponsard et al., 2018). For example, the UK government makes available through its website a self-assessment checklist that later generates an action plan with the aim of improving awareness associated with cybersecurity (UK Government, 2016).

In December 2020, the European Commission and the European External Action Service have proposed a new cybersecurity strategy for the EU, to combat the threats posed by cyberspace and ensure that citizens and businesses benefit from the digital world in a secure way. Thus, proposals for the development of three instruments (i.e., regulatory, investment and policy initiatives), that will report different areas of EU action: "1) resilience, technological sovereignty, and leadership; 2) operational capacity to prevent, detect and respond; 3) cooperation to advance a global and open cyberspace" (European Commission, 2021)

With the arrival of the 5G network, new risks from cyberspace will appear. For this reason, cybersecurity will play an important role to protect the economy and the societies across the world. In this sense, the European Commission on 26 March 2019, recommended to the member states of the UE to focus on this matter and to create a toolbox with the objective of mitigate the new risks brought by the 5G network.

To implement the toolbox, the risks that UE need to have in mind were identified and categorized according to their degree of importance, making it possible to apply the best guidelines and measures to mitigate the identified risks. The risks were categorized into 5 categories, namely: (1) Risks associated to inadequate security measures; (2) Risks associated to 5G supply chain; (3) Risks associated to the behavior of individuals or organizations; (4) Risks associated with independencies between 5G network and other fundamental systems; (5) Risks associated to end user devices. After that, two types of measures to mitigate the mentioned risks have been defined: Strategic (which are mainly measures related to the increase of regulatory powers regarding the authorities to oversee the acquisition and deployment of the networks and measures related to non-technical vulnerabilities) and technical (measures that are aimed to increase the security of 5G networks and equipment). Thus, 8 strategic measures and 11 technical measures have been identified.

The **strategic measures** are as follows: (1) Reinforcement the role of the national authorities; (2) Execute audits on operators and requiring evidence; (3) Assess the risk of suppliers and apply restrictions; (4) Monitoring the consumption of managed service providers and equipment suppliers' third line support; (5) Safeguarding the variety of suppliers for individual mobile network operators through adequate multi-vendor strategies; (6) Reinforcement the resilience at national level; (7) Recognizing crucial assets and fostering a varied and sustainable 5G ecosystem in the EU; (8) Sustaining and constructing diversity and EU capacities in future network technologies.

The **technical measures** are as follows: (1) Safeguarding the application of basic security requirements; (2) Safeguarding and assessing the employment of security measures in existing 5G standards; (3) Safeguarding strict access controls; (4) Improve the security of virtualized network functions; (5) Safeguarding safe 5G network management, operation and monitoring; (6) Improving physical security; (7) Improving software update, integrity and patch management; (8) Improve the security standards in the suppliers processes through more demanding conditions; (9) Require EU certification for 5G networks in different aspects (e.g., customer components); (10) Require EU certification for non-5G-specific information and communication technologies products and services; (11) Safeguarding resilience and continuousness plans (2020).

According to previous research (Spruit, 2014) (Mijnhardt et al., 2016), it is necessary to meet certain requirements during the development process of a new model that is suitable for assessing and improving cybersecurity in SMEs. The below summarizes the requirements needed to adopt:

**Table 4 - Requirements to design a new model**

| | |
|---|---|
| **User friendly \|Self-evalution** | It is crucial that SMEs can easily carry out evaluation planning and improvements without the need for extra resource use. |
| **Situational consciousness** | During the process of developing the model, it is necessary to take into account the characteristics of the organizations. Thus, it is important that the model provides personalized guidance and an implementation plan. |
| **Transparency with the standards** | The must comply with existing standards in cybersecurity. |
| **Cybersecurity awareness** | It is important that the model provide training material and have the capability to increase awareness in cybersecurity. |
| **Maintainability** | Cybersecurity is an area in constant evolution, so it is necessary that the model allows adjustments according to the implementation of new standards or techniques. |

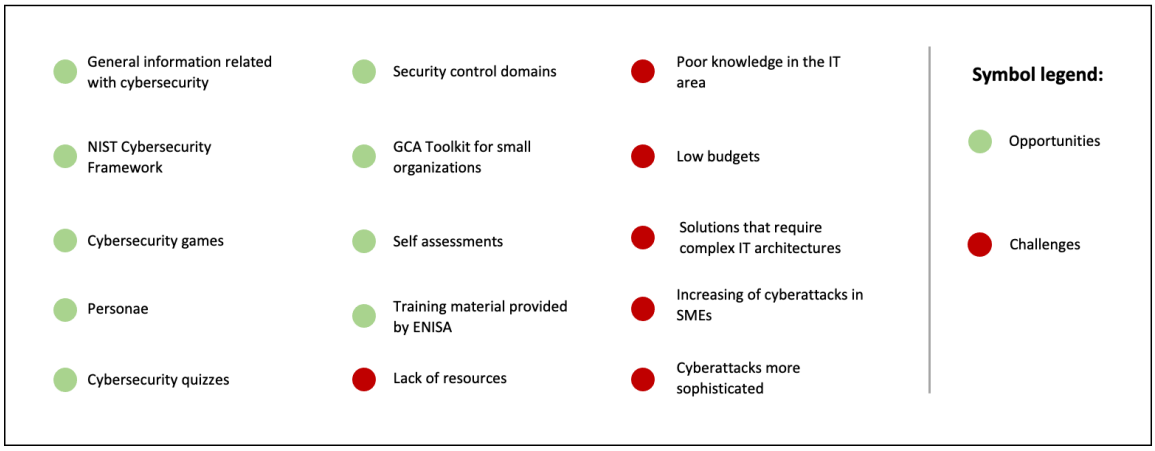
Based on the information obtained throughout section 3.1, it is possible to summarize certain opportunities and challenges for the development of the cybersecurity toolbox for SMEs.

Consequently, regarding the **challenges** associated with cybersecurity in SMEs, it is necessary to highlight the following: as it was possible to observe throughout the section 3.1, SMEs showed different weaknesses, namely the lack of resources, poor knowledge in the IT area, low budgets and the fact that incentives created are more linked to the large companies. In this sense, it is necessary to consider the weaknesses present in SMEs, for the development of the security toolbox. Another challenge to be pointed out is the fact that there are several solutions that require complex IT architectures, which from the perspective of SMEs is seen as negative given the lack of knowledge and resources. Finally, it is necessary to highlight the fact that the number of cyberattacks on SMEs is increasing and it is more difficult to detect or respond to certain attacks. Therefore, it will be essential to consider the different control measures proposed in the ISO/IEC 27002:2013 described in the section 3.1.2.

Regarding the identified **opportunities,** it is possible to emphasize the following: throughout section 3.1, it was possible to verify different techniques and tools that help SMEs mitigate some risks present in cyberspace and to increase the awareness associated with cybersecurity. Thus, for the development of the security toolbox we will consider different techniques and tools. As a key tool, we will take into account the toolbox developed for SMEs by Global Cyber Alliance and trying to reinforce it with other techniques and information founded, namely, quizzes, self-assessments, personae, games, the training material proposed by ENISA, the NIST cybersecurity framework, the free cybersecurity tools proposed by Johnson and some control measures provided in the ISO/IEC 27002:2013. We will only consider certain control measures proposed by ISO/IEC 27002:2013 regarding the complexity of the 14 security controls and the challenges identified in SMEs. In the light of the above explanations, the following security controls domains were considered: 1) information security policies; 2) human resource security; 3) asset management; 4) access control; 5) physical and environmental security; 6) operations security; and lastly, 7) communications security.

The figure bellow summarizes the challenges and opportunities identified that will be considered to design the security toolbox.

**Figure 7 - Challenges and opportunities**




In the next phase, based on the opportunities and challenges founded, a Systematic Literature Review was carried out following the PRISMA methodology.

## 3.2. SYSTEMATIC LITERATURE REVIEW

As mentioned in the section 2.2, systematic literature review process will allow the identification of gaps to design the security toolbox, according to defined research questions and the selected exclusion and inclusion criteria. Thus, the PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) Statement will be adopted.

For the systematic literature review, the following research questions were used as a basis for research initiation:

1. What are the risks associated with cybersecurity that SMEs need to face?
2. What are the cybersecurity techniques and tools available in the market that impact SMEs?
3. How can SMEs mitigate the risks associated with cybersecurity?
4. How to raise cybersecurity awareness in the SMEs?

In the next stage, it is necessary to obtain answers to the above-mentioned research questions. In this sense, inclusion and exclusion criteria were defined to improve the quality of our research:

**Table 5 - Inclusion and exclusion criteria to the systematic literature review**

| **Inclusion criteria:** |
|---|
| **Databases:** ESBCO |
| **Period range:** From 2015 |
| **Keywords:** "Security Toolbox AND SMEs", "Cybersecurity Awareness AND SMEs", "Cybersecurity Risks and SMEs" and "Security Techniques AND SMEs" |
| **Topic adherence:** must contain SMEs environment that contribute with techniques and methods to improve cybersecurity practices and behaviors |
| **Exclusion criteria:** |
| **Language:** Not in English |
| **Format:** Not available in PDF format |
| **Access:** Not available as full text |

Using the ESBCO database, boolean queries were created to include the keywords defined in the Table 5. The first boolean query tested aimed to look for information in all fiels in the articles, and it was the following:

***"TX (cybersecurity awareness AND SMEs) OR TX (security techniques AND SMEs) OR TX (cybersecurity risks AND SMEs) OR TX (cybersecurity toolbox AND SMEs)"***

In this sense, it was obtained a total of 43,427 articles. Then, using Microsoft Excel, we excluded from our sample 10,000 duplicated articles.

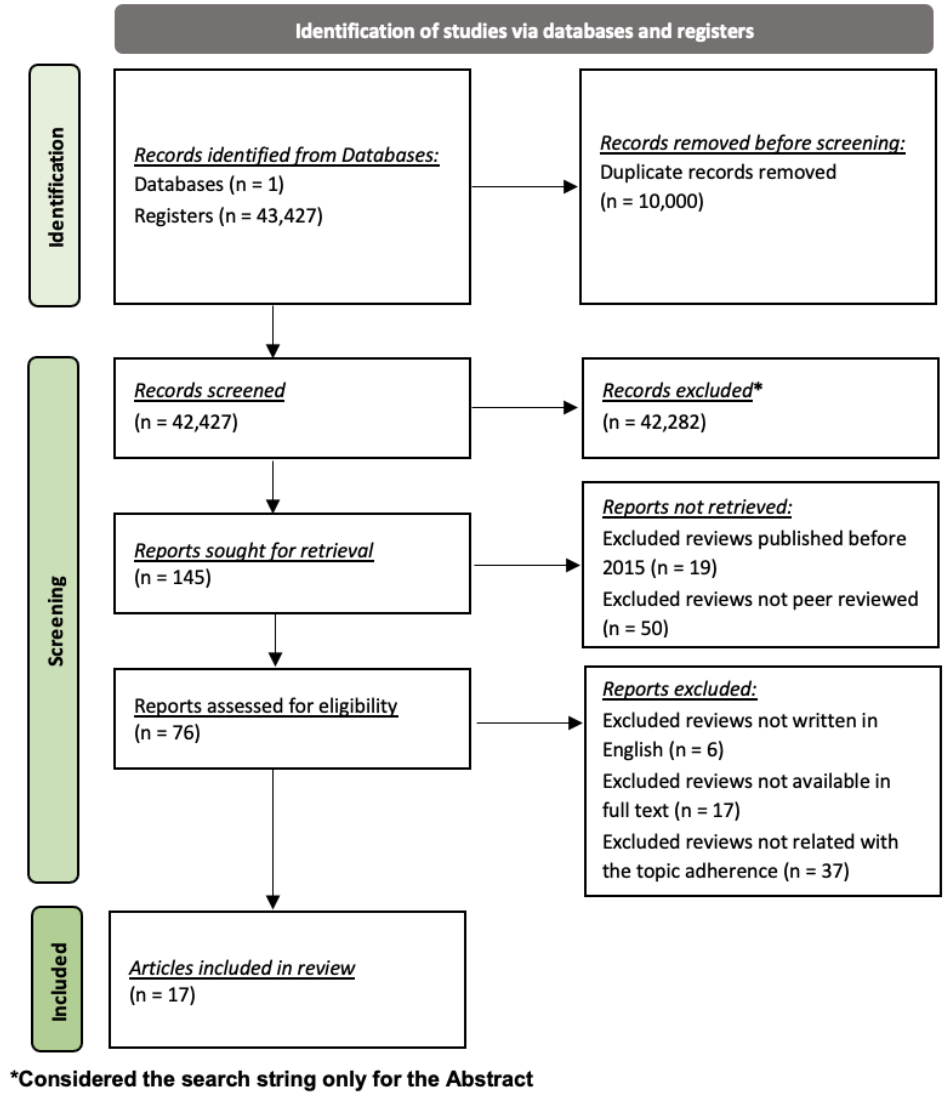
To reduce the sample obtained, the same boolean query was used, but aimed to look for information exclusively in the abstract. Thus, with the application of this criterion, a sample of 145 articles was obtained.

In the next step, all articles that were published before 2015 were excluded, with the aim of obtaining the most recent information. Additionally, articles that were not peer-reviewed were excluded to ensure the quality of the articles selected. By applying the described criteria, a sample 76 articles obtained.

In the next phase, the 76 articles were analyzed. Thus, 6 articles were rejected for not being written in English, 17 articles for not being available in full text and 37 articles for not contributing with techniques or methods to improve cybersecurity behaviors and practices in SMEs. Furthermore, using Scimago, we quantified the ranking of the journals that publish the selected articles.

In the figure below represents the PRISMA flow, that explains in a summarized way the different phases (identification, screening and included) that occurred in the article selection process, as well the number of articles that met the search criteria defined in the Table 5 and the number of articles that were excluded until obtaining our final sample to be considered.

**Figure 8 - PRISMA Flow Diagram - Adaptation** (Page et al., 2021)



Thus, according to the strategy described, 16 essential articles were selected to answer the research questions raised.

**Table 6 - Articles included in the systematic literature review**

| Authors | Title | Resume |
|---|---|---|
| (Armenia et al., 2021) | A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs | Due the increase of threats present in cyberspace, it becomes necessary to assess the risks associated with cybersecurity and create effective investment strategies. In this sense, a framework was created by NIST to help organizations manage the risks associated with cybersecurity. However, the Framework proposed by NIST does not follow organizational changes or changes in the environment (e.g., cyberattacks). Additionally, as it is a complex framework, it becomes difficult to implement in SMEs due their low qualification in the IT area. Thus, the framework proposed with the objective of supporting SMEs in their investment decisions based on the assessment of risks associated with cybersecurity. The framework aims to dynamically access the profile of organizations to be useful in the long term. Lastly, it was possible to demonstrate the ability to assess the profile status of SMEs related with cybersecurity and assess the impacts of investments, increasing the awareness associated with security. |
| (Alahmari & Duncan, 2020) | Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence | Nowadays, there have been strong incentives for SMEs take advantage of new opportunities available in the market by adopting new technological solutions. However, SMEs do not give the necessary importance to the threats associated with cybersecurity, which it is translated in increase of risks and vulnerabilities. In this sense, a systematic literature review was carried out with the aim of collect evidence related with importance of the management role in SMEs regarding the different threats and risks present in cyberspace. It was possible to conclude different perspectives, namely, the importance of threats, behaviors, practices, awareness, and decision making. Lastly, it is mentioned that for future work an empirical research on different risk management methods associated with cybersecurity in SMEs is relevant. |

| Authors | Title | Resume |
|---|---|---|
| (van Haastrecht et al., 2021) | Respite for SMEs: A Systematic Review of Socio-Technical Cybersecurity Metrics | Currently, the threats associated with cybersecurity are a reality for SMEs and organizations need to have this in mind. Thus, to mitigate the threats mentioned, it is important that SMEs make an assessment of their profile associated with cybersecurity. However, it is possible to identify some challenges, namely in the complex socio-technical content of SMEs. In this sense, the aggregation of metrics and adaptability of solutions have been debated issues, as they are important topics for SMEs given their difference needs. Based on a systematic literature review, it was possible to conclude that there is a need to create new intuitive risk assessment approaches based on the threats associated with cybersecurity that SMEs must deal with. |
| (Benz & Chatterjee, 2020) | Calculated risk? A cybersecurity evaluation tool for SMEs | SMEs are the most vulnerable companies and the most exposed to the risks associated with cybersecurity. Despite its usefulness in terms of evaluation, the Cybersecurity Framework proposed by NIST does not meet all the needs of SMEs. In this sense, a new methodology is proposed, which is an evaluation tool. This tool is divided into 35 questions for SMEs carry out a self-assessment of their maturity in five categories present in the Cybersecurity Framework proposed by NIST, specifically, identify, protect, detect, respond, and recover. |

| Authors | Title | Resume |
|---|---|---|
| (Löffler et al., 2021) | CySecEscape 2.0 – A Virtual Escape Room to Raise Cybersecurity Awareness | Over the years, SMEs have been increasing their presence in digital world, which translates into an increase in risks associated with cybersecurity and an increase in cybercrime. According to previous studies, it was possible to verify that humans have been the main responsible for the vulnerabilities associated with cybersecurity. Thus, it is clear, that training in cybersecurity is essential to raise awareness among employees on this topic. In this sense, the existence of escape rooms experiences was reported as technique to increase cybersecurity awareness. Taking into account the current paradigm caused by the pandemic, a prototype was developed for a virtual escape room solution addressing the different challenges associated with cybersecurity present in SMEs. |
| (Rawindaran, Jayal, & Prakash, 2021) | Machine Learning Cybersecurity Adoption in Small and Medium Enterprises in Developed Countries | In several developed countries, the use of AI and ML have been useful to manage and protect data in organizations. In view of the recent changes in the UK GDPR, Brexit and the requirements of ISO standards, ML has become essential to adopting cybersecurity and can be seen as an example for other developed countries. However, there are still many SMEs that are not adopting this technique. In this sense, the different challenges to adopt machine learning associated with cybersecurity in SMEs are reported. Furthermore, barriers and reasons for the low adoption rates of this techniques in SMEs are highlighted. Additionally, based on the study carried out, it was possible to perceive that SMEs have several tools at their disposal, but do not have the essential knowledge for their correct use. Thus, it was possible to conclude that the lack of knowledge on the part of SMEs can be resolved with training to employees gain awareness of appropriate security measures. |

| Authors | Title | Resume |
|---|---|---|
| (Park et al., 2021) | 7S Model for Technology Protection of Organizations | Currently, the new technologies have a strong importance for the vast majority of organizations, so cyberattacks can cause considerable financial losses. Organizations use protection tools to mitigate the risks associated with cybersecurity however SMEs face some difficulties in using these tools due the complexity. Thus, a diagnostic model is proposed to assess the protection capabilities of organizations based on the individual ements of the 7S Model: shared values, strategy, structure, systems, team, style and skills. |
| (Lanz & Sussman, 2020) | Information Security Program Management in a COVID-19 World | Over the years, cybersecurity has been a major concern for some companies. In 2020, with the emergence of the Covid-19 pandemic, new challenges and risks emerged, forcing most organizations to undergo restructuring in their business models. Thus, the article aims to identify the main problems that the pandemic has brought to SMEs and the necessary steps to implement efficient cybersecurity programs. Additionaly, resources are identified that SMEs can take advantage to implement and monitor the performance of employees related to cybersecurity. |
| (Aigbefo et al., 2020) | The influence of hardiness and habit on security behaviour intention | SMEs have a strong importance in Europe, which makes them a strong target for cybercriminals. Thus, in the present study, the various factors that influence the security behaviors of SMEs employees are investigated to understand how SMEs can manage the risks associated with cybersecurity. Based on a study carried out with 294 employees, it was possible to conclude that personality traits and resistance habits have a significant impact on the intentions of security behaviors on employees. The different threats associated with cybersecurity can lead to unconscious responses by employees, hence the importance of developing adequate safety habits. Additionally, it has been found that successful cyberattacks often result from psychological manipulation of employees with susceptible personality traits and low security habits. In this sense, it is concluded that the level of robustness in SME employees increases the probability of promoting adequate safety habits. |

| Authors | Title | Resume |
|---|---|---|
| (Mitrofan et al., 2020) | DETERMINING THE MAIN CAUSES THAT LEAD TO CYBERSECURITY RISKS IN SMES | The new technologies can be considered an enabling lever in the development of SMEs, but there are also many associated risks. Thus, in this study, the main concerns of managers in relation to cybersecurity and the main causes of risks associated with cybersecurity in SMEs are identified. In this sense, it was possible to conclude that there is a strong need to improve the defense structure against cyberattacks in SMEs. Additionally, it is concluded that there is a low level of preparation for the different threats associated with cybersecurity since it is a dynamic environment and SMEs do not make the necessary investments for an adequate cybersecurity structure. |
| (Lopez et al., 2020) | Intelligent Detection and Recovery from Cyberattacks for Small and Medium-Sized Enterprises | Cyberattacks are a major threat to computer security in companies. These attacks have evolved over the time, becoming more sophisticated and robust. Given their characteristics and structure, SMEs have been greatly harmed by cyberattacks. However, it is worth mentioning that SMEs, given the low levels of economic resources, experience greater difficulties in implementing solutions to combat the risks associated with cybersecurity. Thus, it is understood that it is necessary to create affordable security solutions for SMEs capable of detecting and recovering from cyberattacks. In the present study, a cybersecurity platform is proposed with the mission of making SMEs systems safer. The proposed platform combines the application of proactive security techniques with machine learning and blockchain, allowing security in the different phases of a cyberattack. Thus, it is concluded that the tool helps SMEs in the prevention phase by preventing systems for being attacked; in the detection phase, allowing the identification of potentially harmful situations for the systems; in the containment phase, trying to stop the effects of a cyberattack; and in the response phase, helping to recover infected systems. |

| Authors | Title | Resume |
|---|---|---|
| (Kim et al., 2019) | A big data framework for network security of small and medium enterprises for future computing | It was reported that control systems of SMEs in most cases do not consider threats associated with cybersecurity, which leads to these organizations being more exposed to the risks in cyberspace. Thus, a method is proposed to increase the security capacity of SMEs, especially for big data applications. The proposed method's mission is to allow SMEs to carry out security reviews through mobile devices. Additionally, it is expected that in future studies, the application will make some code available to SMEs through Open Source to contribute to the strengthening of their security capabilities. |
| (Bada & Nurse, 2019) | Developing cybersecurity education and awareness programmes for small and medium sized enterprises (SMEs) | The article aims to propose a program to educate and make SMEs aware of cybersecurity because it is an essential component for an effective cybersecurity strategy. Based on the approach adopted, it was possible to perceive the variety of existing programs and that are opportunities for improvements, in order to lead to a program of high level of education and awareness of cybersecurity. |
| (Archibald & Renaud, 2019) | Refining the PoinTER "human firewall" pentesting framework | In this article, penetration tests are identified as a useful tool to detect vulnerabilities that exist in an organization. Over the years, the human has gained greater importance in the organization because it is necessary to ensure that they are resistant to cyberattacks. Thus, there are organizations that test their employees through their resilience and their ability to detect and repel cyberattacks. According to previous studies, a human testing tool (PoinTer) adapted to SMEs was identified. However, in the article is defended that the tool is subject to improvements derived from ethical principles. In this sense, the compliance of the tool with GDPR is proposed. |

| Authors | Title | Resume |
|---|---|---|
| (Goode et al., 2018) | Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness | Organizations are increasingly dependent on new technologies, which causes an increase in cyberattacks. The humans, due their lack of knowledge and skills in this matter, are considered the main risk factors associated with cyberattacks. Thus, based on previous studies, it was possible to verify that awareness techniques are the first step to adopt, to increase the levels of cybersecurity knowledge. The study reports that despite the different training initiatives present in many organizations, there are a limited number of empirical studies that focus on security education, training, and awareness programs. In this sense, the study had the following objectives: identify the topics necessary to implement an education, training, and awareness program; identify awareness measurement criteria; and identify the different contents in programs related with integrated assessment systems. |
| (Franco et al., 2020) | SecBOT: a Business-Driven Conversational Agent for Cybersecurity Planning and Management | In recent years, organizations have been increasing their presence in the digital world, which gives rise to new threats, namely issues associated with cybersecurity. In this sense, to mitigate the negative effects associate with these threats, some companies have made investments to improve their security structure. However, SMEs have low budgets, low technical knowledge, and few employees to deal with the issues associated with cybersecurity. Thus, it is essential to develop new approaches to provide technical information related to cybersecurity. This article identifies a chatbot (SecBot) that supports cybersecurity planning and management. Through the application of neural networks and natural language processing (NLP), SecBot allows the identification of cyberattacks based on certain symptoms, the identification of solutions and configurations according to the organization's environment and provides information for decision making about investments and risks associated with cybersecurity. |

| Authors | Title | Resume |
|---|---|---|
| (Fielder et al., 2016) | Decision support approaches for cyber security investment | When investing in cybersecurity resources, it is important for managers to pay attention to certain decision-making strategies. Thus, three decision support methodologies are identified (one based on game theory, another based on combinatorial optimization and finally one based on a hybrid methodology). The purpose of the study is to identify weaknesses and strengths of the different cybersecurity investment methodologies mentioned. To compare the different methodologies, a decision support tool was developed and a case study on current government guidelines, was developed. Additionally, the importance of the proposed tool in supporting decision-making regarding the protection requirements against cyberattacks in SMEs is reported. |

With the information obtained, it is necessary to discuss the different assumptions present in the 16 articles identified through the systematic literature review. Based on the assumptions, it will be possible to propose the development of a useful toolbox for SMEs according to the scientific knowledge acquired throughout the section 3.

Furthermore, it should be noted that based on the research carried out in this chapter, it was possible to draw conclusions considered the research questions, namely, the various risks that SMEs need to face related to the cyberspace, the different techniques and tools available on the market, the ways that managers can raise cybersecurity awareness in SMEs and how SMEs can mitigate the risks associated with cybersecurity. However, it should be highlighted that based on the literature review carried out, it was not possible to quantify the impact that the different tools and techniques, described throughout chapter 3, have in SMEs.

With this, in chapter 4 the assumptions obtained will be presented in greater detail based on the literature review conducted.

# 4. PROPOSAL

In this chapter, based on the findings of research background described on previous chapter, we will propose a Framework to mitigate the risks of cyberspace.

## 4.1. ASSUMPTIONS

Based on the systematic literature review conducted in section 3.2, it was possible to conclude certain assumptions, that will be considered for the proposal of a framework to mitigate the risks of cyberspace, namely:

**Main weaknesses of SMEs in cybersecurity**

According to the literature review, it is possible to notice that there is a lack of awareness in SMEs regarding the cybersecurity, which leads to increased risks of cyberattacks.

Furthermore, another aspect to be highlighted is the lack of preparation of employees in SMEs, i.e., employees do not know what behaviors they should have to mitigate the risks of cyberattacks. This lack of preparation is caused by the poor investment in security.

Another issue that deserves to be emphasized it is the difficulty of SMEs to carry out an assessment of their cybersecurity profile considering their different needs.

Additionally, it is important to point the fact that there are several solutions that require complex IT architectures, which from the perspective of SMEs is seen as negative given the lack of knowledge and resources.

Finally, it is necessary to highlight the fact that the number of cyberattacks on SMEs is increasing and it is more difficult to detect or respond to certain attacks. This situation was intensified with the emergence of the Covid-19 pandemic that forced most organizations to undergo restructuring in their business models.

Against this background, it was possible to conclude through the literature review that the causes that can lead to a cyberattack in SMEs are several, however, if employees were aware of the dangers of cyberspace the risks of possible cyberattacks could be reduced.

**Methods of raising cybersecurity awareness in SMEs**

According to several studies mentioned in the literature review, it has been possible to conclude that making employees aware of cyberspace risks is a key factor for SMEs be successful and less exposed.

Based on the literature review it was possible to verify the existence of a chatbot that support cybersecurity planning and management. Additionally, the chatbot allows the identification of cyberattacks based on certain symptoms, the identification of solutions and configurations according to the organization's environment and provides information for decision making about investments and risks associated with cybersecurity.

An alternative technique that could be useful to increase cybersecurity awareness is the is the use of escape rooms that address different challenges associated with cybersecurity present in SMEs.

Additionally, it is important to consider the organization's security policies when implementing a security education, training and awareness program. As stated by Goode, Levy, Hovav and Smith, the main topics and subtopics that should be included in the mentioned program are:

- Data security (e.g., privacy, physical and environmental security, data backup and storage, data loss and data regulations);
- Common risks and vulnerabilities (e.g., phishing and vishing, malware, software restrictions, spam, ransomware and safe browsing);
- Accessing work systems (e.g., mobile security, working remotely, bring your own device and cloud); and,
- Password management (e.g., password security and creating strong passwords).

**Mechanisms of detection and defense**

As seen in previous studies, SMEs invest in different security measures that are not effective to protect them from the different risks of cyberspace. In this sense, it is important that organizations have in place security systems that allow to detect effectively threats, in a way that prevent serious losses for the organization.

Some examples of security systems are: (i) Security Operations Centers (SOCs); (ii) Managed Security Service Providers (MSSPs); (iii) Intrusion Detection Systems (IDSs); and, (iv) Security Information Event Management (SIEM) systems.

However, the examples listed above require some financial capacity and for this reason it is difficult for SMEs to acquire this security solutions. Thus, according to different studies, the following could be concluded:

- To **prevent** from the risks of cyberspace, SMEs should implement security systems that include self-backup, self-update, and access control. Additionally, it is important to implement firewalls and anti-malware solutions;
- To **detect** threats and attacks, SMEs can use some machine learning algorithms to detect intrusions and the most affecting attacks (e.g., decision trees or random forecast). Consequently, micro-services must be employed to detect each of the attacks that can connect with the employers using an Application Programming Interface (API);
- To **contain** an attack and mitigate the impact, the SMEs could create a virtual environment that must be implemented to cheat the hackers. This virtual environment it is based on deception technology;
- To **recovery**, it is important to take the following steps: (i) create a Security Incident Response Plan (SIRP); and (ii) implement self-recovery procedures. For that, SMEs must implement a recovery system that include a list of malicious IP addresses.

Another technique mentioned in the study performed by Archinald and Renaud to detect vulnerabilities is the penetration test (i.e., the simulation of an authorized cyberattack, to assess the security of an organization). In this sense, the key techniques in penetration tests are:

- **"Phishing" employees:** this technique will allow to understand if the employees will click on a certain or attachment;
- **Cloning websites:** this technique will permit to understand if the employees will give their personal credentials to a particular website;
- **Request for information:** this technique will allow to know how much information it is possible to obtain from employees via the phone, online or in-person;
- **Assess physical security:** this technique will permit to understand if there are difficulties in entering on the premises of a company;
- **Media drop**: this technique will allow to know if employees plug a USB cable on their work computers.

## 4.2. TOOLBOX

Considering the assumptions exposed in the section 4.1, it becomes possible to present the proposed in this research, i.e., a security toolbox for SMEs capable to identify, protect, detect and respond to potential cyberattacks. The implementation of a security toolbox that helps SMEs may be relevant and can provide great results for different organizational environments to mitigate the risks of cyberspace.

The suggested framework would play an important role, to the users of the security Toolbox to get more know-how to protect the business environment.

Substantially, the security toolbox (hereinafter "+Secure") will be a virtual environment with four distinct areas (identify, protect, detect and respond). In the different areas, support material and tips will be available to make possible for SMEs employees adopt an adequate behavior to mitigate the risks of cyberspace.

**Identify**

In the first step, a checklist is given for the workers to carry out an inventory of their devices (e.g., laptops, smartphones, printers, and others.), of their applications (e.g., businesses applications, online accounts, and others). In addition, some tools will be suggested by the +Secure to help employees to take the inventory of their devices and applications, for example, thought the "Fing app" or "CIS Hardware and Software Asset Tracker Spreadsheet".

Then, based on the identification of applications and devices, it is important to understand the cybersecurity risks present in the company. On the basis of the foregoing considerations, the +Security will suggest different tips and tools that will help workers in this task (e.g, may be suggested the "SecurityScorecard"). It should be noted that this tool will allow employees to track the risks taking into account the devices and applications in use, and receive alerts in case of vulnerabilities for the security of the company.

**Protect**

In this area, the +Secure will provide tips and support material to help SMEs protect themselves against cyberattacks.

In the first module of this area, the +Secure will suggest to update the defenses (i.e., it is necessary for SMEs to have their systems, devices and data updated). It should be noted that the software developers regularly release security updates with the aim of resolving identified vulnerabilities that could compromise users' safety. Considering the aforementioned, +Secure will address the need for timely system updates. When the systems are no longer supported by manufacturers/software developers, the Toolbox will send alerts to employees to remove them, through the fact that those systems cannot be updated anymore.

Additionally, the +Secure will provide tools to guide SMEs to configuring systems and applying updates automatically (e.g., Auto-update Apple or Auto-update Windows).

In the second module of the protect area, the +Secure will suggest that SMEs encrypt their data as it makes it more difficult for cybercriminals to access it. Thus, the +Secure will provide some solutions that will help SMEs to encrypt their data, e.g., could be suggested the PGP for encrypting email or BitLocker for Microsoft Windows that is a protection feature the encrypts drives on Windows servers.

In the third module of this area, the +Secure will provide different tools to help SMEs protect their websites against hackers that could gain access to the company website. For example, the Toolbox will

suggest the “Let’s encrypt” for SMEs get a digital certificate to enable HTTPs on their websites and the “Immuniweb” that allows SMEs scan their websites and find weaknesses.

**Detect**

As previous mentioned in section 4.1, SMEs have been an increasing target by cyberattacks. The most common attacks are through malwares or phishing attacks. This type of cyberattacks can cause serious damage to SMEs, so it is necessary to adopt measures to detect these attacks.

In view of the above, in the third area of +Secure some tools and tips will be available that will allow SMEs employees to detect these cyberattacks. Thus, +Secure will suggest the following tools:

- **Anti-virus:** in this category, the toolbox will suggest to employees installing a real time antivirus on their devices to detect the virus and to mitigate the risk of affecting the device. In addition, it will be suggested to activate Microsoft Defense.
- **Ad Blockers:** for block some online advertisements or messages that could appear while an employee browsing through a website, the +Secure will suggest the installation of ad blocker for different browsers (e.g., chrome, edge, Firefox and Safari) in order to offer additional protection on the internet.
- **Domain Name System (DNS) Security:** taking into account that some cybercriminals try to trick their victims through an untrustworthy website, the toolbox will suggest the installation of DNS firewalls (e.g., Quad9) that checks if the IP address of the website is secure.

Furthermore, +Secure will suggest the implementation of DMARC (Domain- based Message Authentication, Reporting & Conformance) that will help SMEs to identify potential lookalike domains. With the DMARC, SMEs will receive daily reports that shows if the email of the employees is being used for another person. In this sense, it is understood that this policy will allow SMEs to be more quickly in the detection of fraudulent behaviors.

**Respond**

During a cyberattack it is important that SMEs know how to react and have implemented policies to combat them.

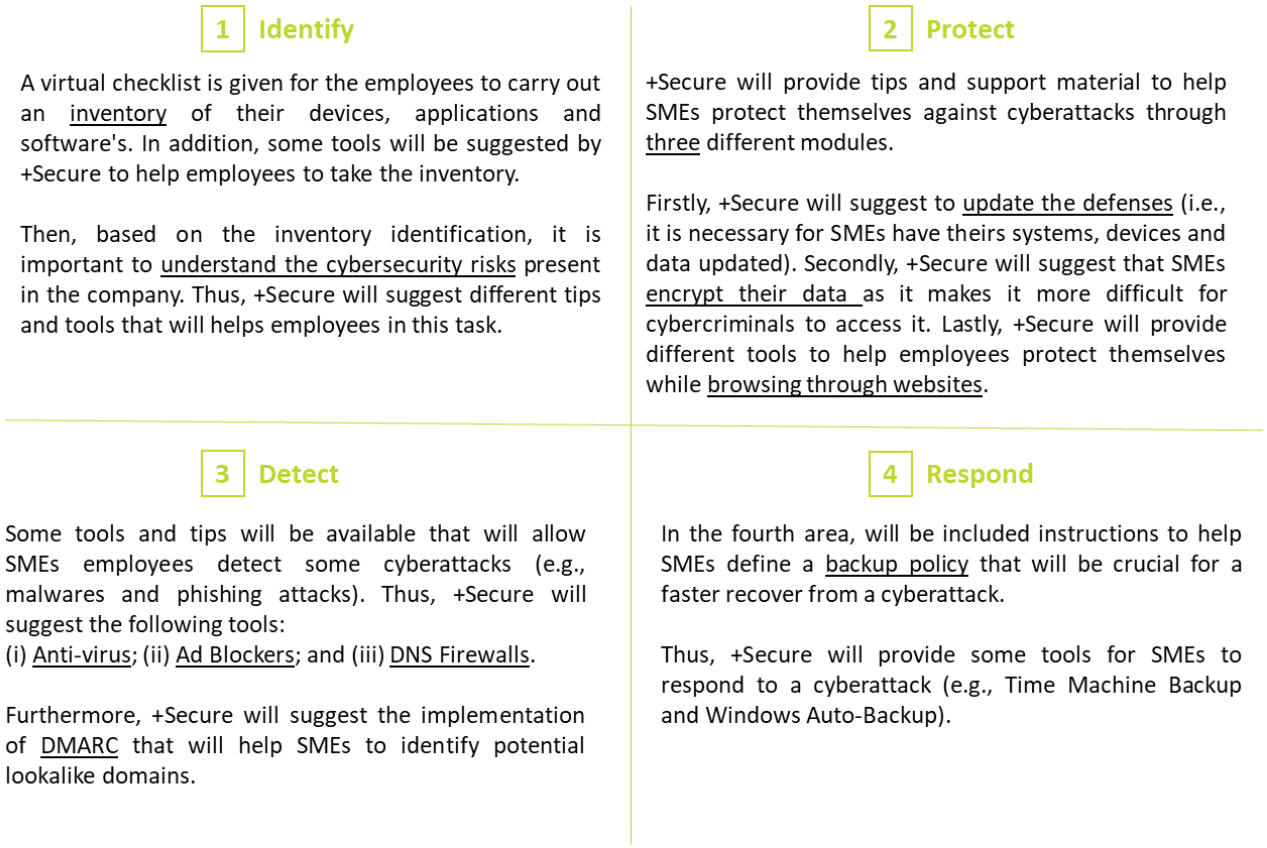
Last but not least, in the fourth area, will be included instructions to help SMEs define a backup policy that will be crucial for a faster recover from a cyberattack.

The implementation of a backup policy will allow to SMEs mitigate the negative effects (i.e., loss impact of reputational, financial or legal) of an attack, for example, it could help in recovery from data corruption or data loss.

Thus, +Secure will provide some tools for SMEs to respond to a cyberattack, namely: (i) Time Machine Backup (a toll for employees set up automatic backups on their Mac operating systems; or (ii) Windows Auto-Backup (a tool for employees set up automatic backups on their Windows operating systems).

The figure below summarize the proposed toolbox.

**Figure 9 – Proposed toolbox for SMEs**



# 5. EVALUATION /DISCUSSION

In this section, an use case of the proposed toolbox was described, and a discussion was carried out with experts in the field of cybersecurity with the aim of evaluate/validate the prosed Toolbox.

## 5.1. USE CASE

In this section, it will be presented an use case with the aim of demonstrate the utilization of the +Secure in the organizational environment.

### 5.1.1. Toolbox application example

It should be noted that the company (hereafter "XPTO" or "Company") described below for the use case is a fictitious company.

**Company description**

XPTO is an auditing and consulting company, based in Lisbon. Since 2015, it has contributed to the development of its customers' business. Currently, XPTO has 45 employees and provides the following services:

- Accounting, tax, consulting and related services;
- Investment projects and implementation of quality systems;
- Evaluation and valuation of brands; and,
- Financial audits.

XPTO has a small IT Department (5 employees) and is responsible for ensuring the creation and implementation of technological solutions capable of increasing business productivity, guaranteeing information security and implementing the necessary infrastructure for the operations of the Company.

Considering the increase of cyberattacks in the world, the IT department recently developed a toolbox (+Secure) for the use of XPTO employees. The +Secure has several features that allow employees to identify, protect, detect and respond to potential cyberattacks.

**1.º Step: +Secure configuration**

In September 2022, XPTO received 1 new employee (hereafter "New Joiner") for the tax consultancy team. Considering the policies recently defined by the Company, New Joiner had to configure +Secure on his computer.

New Joiner started by opening the application available on his desktop (pre-installed by the IT department). After opening the +Secure application, a virtual environment appeared with a sequence of tasks to be carried out divided into 4 areas/components: (1) Identify; (2) Protect; (3) Detect; and (4) Respond.

**2.º Step: Go through identify area**

The New Joiner started by opening area 1 – Identify. At this stage, New Joiner had to carry out an inventory of the devices that he uses in the Company, in this case the desktop and the smartphone. Then, a pop-up appeared indicating the installation of the Fing App tool, which allows tracking the devices connected to the XPTO network. After installing and configuring the Fing App, another pop-up appeared with a notice of obligation to keep the inventory up to date regarding the devices, licenses, software and sensitive information in use by New Joiner.

Having made an inventory of the devices and applications in use by the New Joiner, +Secure indicated the installation of the SecurityScorecard. In this sense, the New Joiner after finishing the installation of the SecurityScorecard received a notification with an assessment of the existing risks in relation to the inventory of devices and applications in use by the New Joiner.

In the view of the above, the tasks to be performed by the New Joiner in the first area (Identify) are concluded. Consequently, the New Joiner clicks on the following area available in +Secure – Protect.

**3.º Step: Go through protect area**

Starting the second area, New Joiner notices that it has 3 different modules with tasks to perform. By clicking on the first module, +Secure generates a pop-up with the alert indicating that his devices' (based on the inventory made in the first area) need to be updated and the indication that it is necessary to configure the devices to be automatically updated using Auto-update Windows. Once the tasks in module one is finished, the New Joiner clicks on the second module available in the Protect area.

In this second module, +Secure sends a notification to New Joiner indicating the need to encrypt the data available on its devices using the tools PGP (for email encryption) and BitLocker (to encrypt the data available in the operating system Windows).

After configuring PGP and Bitlocker, the New Joiner goes through to the last available module in the protect area. At this stage, the Toolbox opens a window with a video demonstrating the risks of browsing through the internet and the vulnerabilities that it may bring to XPTO. Upon completion of the video, +Secure generates a pop-up with a new alert that indicates to New Joiner to use the Immuniweb tool in order to test the security of the websites that he browses during its functions as a tax consultant.

**4.º Step: Go through detect area**

Concluded the second area, the New Joiner can start the third area, i.e., the Detect area. After navigating to the third area, +Secure generated a notification indicating the installation of three tools capable of detecting possible cyberattacks.

Consequently, New Joiner starts by installing the suggested Anti-Virus, in this case TotalAV that offers real time protection from malwares. In addition, New Joiner configure the suggested DNS Security, i.e., Quad9, which allows to detect if the IP address of the websites that the New Joiner browses within the scope of its functions as a tax consultant is safe. Right after, New Joiner proceeds to the configuration of the AD Blocker, as suggested by +Secure, in order to detect and block online pop-ups that could bring vulnerabilities to XPTO. After installing and configuring the mentioned tools, +Secure created a new alert to New Joiner to configure a DMARC with the aim of detect fraudulent behavior and to protect his email. It should be noted that at this stage, the Toolbox provided a guide to New Joiner with all the necessary steps for configuring DMARC on his desktop.

**5.º Step: Go through respond area**

After completing the DMARC configuration, the last phase of +Secure becomes available – Respond area. After navigating to this last area, +Secure provided a guide explaining the importance and the steps that the New Joiner should keep in mind regarding XPTO's backup policy in order to be able to respond effectively to a cyberattack. After the reading the guide, Toolbox generated a notification for the New Joiner setting Windows Auto-Backup that allows automatic data backups, thus, it is mitigated the negative effects of cyberattack, namely data loss.

After activating Windows Auto-Backup, +Secure generated a certificate for the New Joiner of how it successfully configured it.

## 5.2. INTERVIEWS DESCRIPTION

The toolbox was presented to three specialists. Then, three qualitative questions were asked to them in order to obtain their feedback and assumptions regarding the +Secure.

Should be noted that each expert was interviewed individually. Additionally, each expert was asked to give permission to record the session to allow and facilitate the transcription of the interview.

Each interview was followed by the artifacts presentation and included three questions:

1. Do you consider the proposed framework useful and why? If not, why do you believe it is not?
2. Do you have any criticism towards the proposed framework? Please explain.
3. Would you consider to implement the proposed framework? Please clarify.

### 5.2.1. Data analysis

The table below presents the experts interviewed for the purposed of discussing the proposed framework.

**Table 7 – Experts interviewed**

| Interviewed designation[1] | Company | Job function | Years of experience |
|---|---|---|---|
| Interviewed 1 | PwC Portugal | Information Security Senior Associate | 6 years |
| Interviewed 2 | Integrity | Information Security & GRC Consultant | 15 years |
| Interviewed 3 | SIBS | Penetration Tester | 2 years |

## 5.3. DISCUSSION

The interviews carried out for the evaluation of the proposed toolbox in this master thesis, allowed a discussion regarding the usefulness, contribution and quality of the artifacts presented for the mitigation of cyberspace risks in SMEs.

**Question 1: Do you consider the proposed framework useful and why? If not, why do you believe it is not?**

The interviewees agreed that the proposed framework is useful and essential in the organizational environment.

Interviewed 2 argues that this framework is appropriate for the current reality of the SMEs. If nowadays we see big companies (for example, Vodafone) and public organizations struggling to get their security governance organized and their cybersecurity controls implemented and in proper operation, what to say regarding SMEs.

In addition, interviewed 1 state that this type of solution should also be designed for SMEs, considering that they do not have the same resources as large companies.

Interviewed 3 mentions that the adoption of this type of solutions by SMEs is essential. In most of cases, these types of organizations are not prepared or aware of the various risks that exist in being present in the digital world.

Additionally, interviewed 3 refer that +Secure could be an excellent tool to create the necessary conditions for SMEs to be less vulnerable to possible cyberattacks, considering that the toolbox is in line with the NIST Framework and other security standards.

[1] For legal reasons, the name of the interviewees were not identified in the master thesis.

**Question 2: Do you have any criticism towards the proposed framework? Please explain.**

Regarding the proposed framework, + Secure, interviewed 2 explain that the proposed framework is aligned with other industry security standards. However, interviewed 2 think it would be interesting, +Secure propose as part of the framework a set of SMEs oriented baseline security controls adequate to this type of organizations, which are today increasingly collaborative, informal, geographically dispersed, cloud-based and remote.

In addition, interviewed 2 and interviewed 1 note that it would be interesting adding the function "Recover". By this way, + Secure would have a differentiated proposal for incident management and recovery/continuity.

Interviewed 1, also mention that the selection of tools suggested by +Secure must be chosen with great awareness in order to allow SMEs mitigate risks and not the opposite, i.e., the choice of tools should not bring vulnerabilities in terms of security for SMEs.

Accordingly, with interviewed 3, the DMARC, mentioned in the detect area, could not be a solution to identify potential lookalike domains.

Instead, interviewed 3 argues that is necessary to implement a whitelist/allowlist. Interviewed 3 states that the whitelist is a strategy adopted by cybersecurity teams that approves a list of IP addresses, email addresses and domain names or applications, while rejecting all others that are not part of the list. Thus, cybersecurity teams have been adopting this strategy considering that it is an effective and efficient way to help protect employee devices and company networks against potential cyberattacks harmful to them. Furthermore, interviewed 3 argues that a whitelisting policy may be essential for SMEs as it allows employees to perform their various functions in a safer and more secure environment, bearing in mind that this policy will allow only authorized applications to be executed.

In addition, regarding the respond area, interviewed 3 state that the back-up policy must at least meet two requirements:

- **Encrypted:** that is, an extra security measure that SMEs must adopt to protect their data, considering that it makes it difficult to access them in case the data are stolen or compromised in any way; and,
- **Off-site:** having a copy of data from a particular company's system in a different geographic location (e.g, a different building) in order to ensure greater data security.

Interviewed 1 and interviewed 3 remark that a forensic analysis can create differentiating value at +Secure. They explained that this analysis involves investigating and documenting the causes of a particular security incident in the company.

Last but not least, interviewed 3 warns that SMEs does not have a good security infrastructure nor people with the necessary knowledge and awareness in the area of cybersecurity. Thus, there will be situations that the +Secure will not be enough to respond to more complex situations.

In the view of the described, interviewed 3 suggest implementing an extra service in the toolbox for employees request external support from a cybersecurity team for assistance in order to respond to complex security incidents.

**Question 3: Would you consider to implement the proposed framework? Please clarify**

The interviewees agreed to consider to implement the +Secure in their organizations.

Interviewed 2 states that as a SME business owner, he would need to have a clear cost/benefit view to take a decision on the implementation of this proposed framework due the investment would depend on measuring risk and opportunity.

Furthermore, interviewed 1 argues that she would implement with the necessary tools in the different areas (identify, protect, detect and respond) according to the needs of the company.

Also, Interviewed 1 states to finalize that cyber-attacks are costly, disruptive and a growing threat to business. + Secure could be a good framework to address global cybersecurity challenges and improve digital trust on SMEs.

Interviewed 3 would like to implement the proposed framework. However, interviewed 3 needed to understand if the tools used at +Secure are certified, audited and the toolbox response time to possible vulnerabilities, for example, in a case of a security incident in the company, interviewed 3 would like to understand how fast +Secure would be able to solve the identified problem.

Additionally, interviewed 3 mentions that another point that would take into account was to understand the investment needed to implement +Secure in an organization. Interviewed 3 argues that it is an essential factor for the choice of the framework considering that the financial resources of SMEs are limited.

# 6. CONCLUSIONS

## 6.1. SYNTHESIS OF THE DEVELOPED WORK

Cyberspace is less secure than it was 10 years ago, since there is currently a facility to access vital information on networked computers, and this leads to an increase in cyberattacks. (Mclennan, 2021). Lately, we have verified some losses in organizations caused by cyberattacks, since they are not prepared for these invasions and do not know how to prevent themselves. Just one successful security breach, theft, error, hack or virus attack on a company can result in reputation and financial damage (Gordon et al., 2011).

Cybersecurity has been gaining attention and importance in the research community. Thus, an investigation was conducted to fill this research gap and help SMEs mitigate the risks present in cyberspace.

At the beginning of the present study, the objectives were defined, where the main objective is to propose a framework capable of identify, protect, detect and respond to potential cyberattacks.

Thus, in order to know more detail in the area of cybersecurity, in a first phase, the main concepts associated with cybersecurity were studied (namely, the evolution of its concept, the most common cyberattacks and the concepts of computer security, information security and systems security), as well the main security areas and control techniques defined by ISO/IEC 27002:2013. In addition, the various tools and techniques currently used on the market by SMEs were identified. In this respect, it was possible to conclude several challenges and opportunities to design the proposed framework.

Furthermore, in a second phase, with the aim of carrying out a research more aligned with the objectives of the present study and identifying research gaps, a systematic literature review was accomplish using the PRISMA Statement. Based on the systematic literature review conducted, it was possible to conclude several assumptions, namely, the main weaknesses of SMEs regarding the cybersecurity, some methods of raising cybersecurity awareness in SMEs and mechanisms of detection and defense against cyberattacks, that were considered in the construction of the toolbox that allow SMEs to protect themselves against the various risks associated with cybersecurity.

Therefore, based on the research conducted as described above, it was possible to design a toolbox that allows its users to gain greater awareness and knowledge of how to protect themselves from the different risks of cyberspace through four distinct areas, specifically: (i) identify, (ii) protect, (iii) detect and (iv) respond.

After the toolbox design and detailing how it can mitigate the risks present in the cyberspace, the +Secure was validated with the aim of fulfilling one of the objectives initially defined. The validation/evaluation was carried out with four interviewees, with experience in the area of cybersecurity, which allowed to have a real perspective of the usefulness of the toolbox proposed on the present study.

After the validation, it was possible to validate the usefulness of the toolbox and have a guarantee that SMEs employees will be able to have help in their routine, taking into account that the toolbox provides the essential procedures and tips to be adopted in order to maintain an organizational environment secure and mitigate the different risks of cyberattacks, e.g., reduce the damage caused by cyberattacks.

To conclude, it can be said that the principal objective of the present study was achieved, as it was possible to present and describe a framework useful for SMEs in the sense that it allows them to be less exposed and vulnerable to the various risks associated with cybersecurity.

## 6.2. LIMITATIONS

The limitations are essentially caused by the time and scope of the present study, considering that the investigation was carried out with the aim of completing a master thesis and was driven by its deadline.

Hence, one of the limitations identified in the process of carrying out this investigation was centered on the fact that it was only possible to validate the proposed toolbox with 3 professionals, which can be considered a reduced sample to guarantee the usefulness of the framework. Furthermore, it should be noted that the validation/evaluation of the proposed framework was carried out only with professionals in the cybersecurity area, which means that none interview was carried out with a person in the academic field. Consequently, the lack of theoretical validation may be considered in the present study. In addition, none employee of an SME with no experience in the cybersecurity area was interviewed for the purpose of validating the proposed framework, which could be seen as a limitation given that the adherence of people with no experience was not evaluated.

The interviewees also mentioned the possibility of including other areas in the proposed toolbox, namely, the function “recover” with the aim of the toolbox have a differentiated proposal for incident management and recovery/continuity.

Another limitation to consider is the fact that SMEs do not have a good IT infrastructure or people with the necessary knowledge and awareness in security field. In this sense, it was noticed that the proposed toolbox will not be able to provide a timely response to more complex incidents.

Furthermore, it was possible to perceive with one of the interviewees that the DMARC could not be a solution to identify potential lookalike domains. Instead, the interviewee suggested the use of a whitelist/allowlist.

Lastly, it should be noted that in the present study it was not possible to identify the financial investment necessary to implement the proposed framework in an SME, which makes the decision to implement the toolbox difficult, considering that SMEs administrators need to understand the cost/benefit of the toolbox implementation to the company.

## 6.3. FUTURE WORK

With the aim of creating greater value for the toolbox proposed in this study, it would be interesting to test the insertion of a new area, namely, the function recover. A future work in this area could be important given that it could allow SMEs, through the application of certain procedures, to continue their activity after an incident caused by a cyberattack.

Additionally, it will be important to understand the investment required by SMEs for the implementation of the toolbox. It should be noted that the investment will vary depend on the company's business model. However, certain costs may be estimated regardless of the SMEs business model, considering that certain tools are essential t identify, protect, detect and respond to the various risks associated with cyberspace.

Also, considering the growth and sophistication of cybercrime, a future study will be important and necessary with the consideration on the proposed toolbox of the most recent revision of ISO/IEC/2022.

Last but not least, a future work should be carried out with the aim of understand the respond time of the toolbox to different incidents and in which cases the toolbox will not be able to react due the fact that it is a complex incident.

## REFERENCES


Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, *62*(4), 539–548. https://doi.org/10.1016/j.bushor.2019.03.010

Adeyinka, O. (2008, May). Internet Attack Methods and Internet Security Technology. *2008 Second Asia International Conference on Modelling & Simulation (AMS)*. https://doi.org/10.1109/AMS.2008.68

Aigbefo, Q. A., Blount, Y., & Marrone, M. (2020). The influence of hardiness and habit on security behaviour intention. *Behaviour & Information Technology*, 1–20. https://doi.org/10.1080/0144929X.2020.1856928

Alahmari, A., & Duncan, B. (2020). Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–5. https://doi.org/10.1109/CyberSA49311.2020.9139638

Anderson, J. P. (1972). *Computer Security Technology Planning Study (Volume I)*.

Archibald, J. M., & Renaud, K. (2019). Refining the PoinTER "human firewall" pentesting framework. *Information & Computer Security*, *27*(4), 575–600. https://doi.org/10.1108/ICS-01-2019-0019

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580. https://doi.org/10.1016/j.dss.2021.113580

Arora, A., Nandkumar, A., & Telang, R. (2006). Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. *Information Systems Frontiers*, *8*(5), 350–362. https://doi.org/10.1007/s10796-006-9012-5

Ashik, M. (2019). *Bulding an Effective Cybersecurity Culture Program*. Https://Secureread ing.Com/Building-an-Effective-Cybersecurity-Culture-Program/.

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security*, *27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., Neugebauer, R., Pratt, I., & Warfield, A. (2003). Xen and the art of virtualization. *ACM SIGOPS Operating Systems Review*, *37*(5). https://doi.org/10.1145/1165389.945462

Baykara, M., Gurturk, U., & Das, R. (2018, March). *An overview of monitoring tools for real-time cyber-attacks*. https://doi.org/10.1109/ISDFS.2018.8355339

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evalutation tool for SMEs. In *Business Horizons* (Vol. 63, pp. 531–540). Elsevier.

Cabaj, K., Kotulski, Z., Księżopolski, B., & Mazurczyk, W. (2018). Cybersecurity: trends, issues, and challenges. In *Eurasip Journal on Information Security* (Vol. 2018, Issue 1). Springer International Publishing. https://doi.org/10.1186/s13635-018-0080-0

Canongia, C., & Mandarino, R. (2014). Cybersecurity: The New Challenge of the Information Society. In *Crisis Management*. IGI Global. https://doi.org/10.4018/978-1-4666-4707-7.ch003

Chang, F. (2012). *The Next Wave - The National Security Agency's review of emerging technologies*.

Christen, M., Gordijn, B., & Loi, M. (2020). *The Ethics of Cybersecurity*. http://www.springer.com/series/7761

CIS. (2017). *CIS Controls - Implementation guide for Small and Medium-Sized Enterprises (SMEs)*. Https://Www.Cisecurity.Org/Wp-Content/Uploads/2017/09/ CIS-Controls-Guide-for-SMEs.Pdf.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). *Technology Innovation Management Review Defining Cybersecurity*. www.timreview.ca

*Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures*. (2020). https://www.abiresearch.com/press/abi-research-projects-5g-worldwide-service-revenue.

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *04*(02), 92–100. https://doi.org/10.4236/jis.2013.42011

ENISA. (2019). *Posters for organisations*. Https://Www.Enisa.Europa.Eu/Media/Multimedia/Material/Awareness-Raising-Posters.

ENISA. (2020). *Training material for SMEs*. Https://Www.Enisa.Europa.Eu/Publications/Archive/Training-Material-SMEs.

ENISA. (2021). *ECSM - European Cybersecurity Month*. Https://Cybersecuritymonth.Eu/.

European Commission. (2003). Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises . *Official Journal of European Union*.

European Commission. (2021). *The Cybersecurity Strategy*. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*, 13–23. https://doi.org/10.1016/j.dss.2016.02.012

Figueiró, T. (2021). *Maioria das organizações planeia aumentar despesa com cibersegurança*.

*Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. (2018). https://doi.org/10.6028/NIST.CSWP.04162018

Franco, M. F., Rodrigues, B., Scheid, E. J., Jacobs, A., Killer, C., Granville, L. Z., & Stiller, B. (2020). SecBot: a Business-Driven Conversational Agent for Cybersecurity Planning and Management. *2020 16th International Conference on Network and Service Management (CNSM)*, 1–7. https://doi.org/10.23919/CNSM50824.2020.9269037

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: Interviews and focus groups. *British Dental Journal*, *204*(6), 291–295. https://doi.org/10.1038/bdj.2008.192

Global Cyber Alliance. (2019). *The GCA Cybersecurity Toolkit for Small Business*. Https://Gcatoolkit.Org/Smallbusiness/.

Goode, J., Levy, Y., Hovav, A., & Smith, J. (2018). Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness. *Online Journal of Applied Knowledge Management*, *6*(1), 67–80. https://doi.org/10.36965/OJAKM.2018.6(1)67-80

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, *19*(1), 33–56. https://doi.org/10.3233/JCS-2009-0398

Guasconi, F., Sabatini, G., Papadopoulou, G., Sharkov, G., Oteiza, S., Berens, H., Çifligu, E., Toffaletti, S., Chkhaidze, N., Metchev, Y., Dombach, T., & Haubler, A. (2013). *SME GUIDE FOR THE IMPLEMENTATION OF ISO/IEC 27001 ON INFORMATION SECURITY MANAGEMENT*.

Habib, I. (2008). Virtualization with KVM. *Linux Journal*, *2008*.

Ham, J. van der. (2021). Toward a Better Understanding of "Cybersecurity." *Digital Threats: Research and Practice*, *2*(3), 1–3. https://doi.org/10.1145/3442445

Hevner, A., & Chatterjee, S. (2010). *Design Research in Information Systems* (Vol. 22). Springer US. https://doi.org/10.1007/978-1-4419-5653-8

Hevner, A. R. (2007). A Three Cycle View of Design Science Research. In *Scandinavian Journal of Information Systems* (Vol. 19, Issue 2).

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. In *Source: MIS Quarterly* (Vol. 28, Issue 1). https://www.jstor.org/stable/25148625

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law and Security Review*, *29*(3), 236–245. https://doi.org/10.1016/j.clsr.2013.03.003

'Horne, R., & 'Joyce, S. (2021, February 17). *Simplifying cybersecurity*. S+b, a PwC Publication.

Hruza, P., Perner, J., & Szabo, S. (n.d.). *Cyber-attacks and attack protection*.

Information Security Forum. (2002). *Effective Security Awareness*.

*Information Technology, Security Techniques, Code of Practice for Information Security Management*. (2013). International Organization for Standardization ISO.

ITU. (2009). *ITU-T Rec. X.1205 (04/2008) Overview of cybersecurity*.

Johnson, J. (2021, July 13). *17 free cybersecurity tools you should know about*. Whatls.Com.

Jones, R. A., & Horowitz, B. (2012). A System-Aware cyber security architecture. *Systems Engineering*, *15*(2), 225–240. https://doi.org/10.1002/sys.21206

Kapp, K. M. (2012). *The Gamification of Learning and Instruction: Game-based Methods and Strategies for Training and Education* (Pfeiffer, Ed.; 1st ed.).

Kemmerer, R. A. (2003). Cybersecurity. *Proceedings - International Conference on Software Engineering*, 705–715. https://doi.org/10.1109/icse.2003.1201257

Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers & Security*, *70*, 663–674. https://doi.org/10.1016/j.cose.2017.08.001

Kim, H.-K., So, W.-H., & Je, S.-M. (2019). A big data framework for network security of small and medium enterprises for future computing. *The Journal of Supercomputing*, *75*(6), 3334–3367. https://doi.org/10.1007/s11227-019-02815-8

Kris Lovejoy. (2020). *EY Global Information Security Survey 2020*.

Lanz, J., & Sussman, B. I. (2020). Information Security Program Management in a COVID-19 World. *CPA Journal*, *90*(6), 28–35.

Löffler, E., Schneider, B., Zanwar, T., & Asprion, P. M. (2021). CySecEscape 2.0—A Virtual Escape Room To Raise Cybersecurity Awareness. *International Journal of Serious Games*, *8*(1), 59–70. https://doi.org/10.17083/ijsg.v8i1.413

Lopez, M. A., Lombardo, J. M., López, M., Alba, C. M., Velasco, S., Braojos, M. A., & Fuentes-García, M. (2020). Intelligent Detection and Recovery from Cyberattacks for Small and Medium-Sized Enterprises. *International Journal of Interactive Multimedia and Artificial Intelligence*, *6*(3), 55. https://doi.org/10.9781/ijimai.2020.08.003

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. In *Decision Support Systems* (Vol. 15).

Mclennan, M. (2021). *The Global Risks Report 2021 16th Edition Strategic Partners*. http://wef.ch/risks2021

Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational Characteristics Influencing SME Information Security Maturity. *Journal of Computer Information Systems*, *56*(2), 106–115. https://doi.org/10.1080/08874417.2016.1117369

Mitrofan, A.-L., Mitrofan, A.-L., Cruceru, E.-V., & Barbu, A. (2020). *Determining the Main Causes that Lead To Cybersecurity Risks In Smes*.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *PLoS Medicine*, *6*(7), e1000097. https://doi.org/10.1371/journal.pmed.1000097

Muller, P., Devnani Shaan, Ladher Rohit, Cannings, J., Murphi, E., Robin, N., Illán, S., Aranda, F., Gorgels, S., Priem, M., Smid, S., Bohn, N., Lefebvre, V., & Frizis, I. (2021). *ANNUAL REPORT ON EUROPEAN SMEs 2020/2021*. https://ec.europa.eu/docsroom/documents/46062

O'Flaherty, K. (2019). How gamification can boost cyber security. *Information Age*.

Osborn, E. (2014). *Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs*.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, n71. https://doi.org/10.1136/bmj.n71

Park, H., Yoo, Y., & Lee, H. (2021). 7S Model for Technology Protection of Organizations. *Sustainability*, *13*(13), 7020. https://doi.org/10.3390/su13137020

Paulsen, C. (2016). Cybersecuring Small Businesses. *Computer*, *49*(8), 92–97. https://doi.org/10.1109/MC.2016.223

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Phirke, A., & Ghorpade-Aher, J. (2019a). Risk Assessment of Software Compliances using ISO 27001 Standard. *JASC: Journal of Applied Science and Computations*, *6*(3).

Phirke, A., & Ghorpade-Aher, J. (2019b). Best practices of auditing in an organization using ISO 27001 standard. *International Journal of Recent Technology and Engineering*, *8*(2 Special Issue 3), 691–695. https://doi.org/10.35940/ijrte.B1128.0782S319

Ponemon Institute LLC. (2018). *2018 State of Cybersecurity in Small & Medium Size Businesses*.

Ponsard, C., & Grandclaudon, J. (2020). Guidelines and Tool Support for Building a Cybersecurity Awareness Program for SMEs. In P. Mori, S. Furnell, & O. Camp (Eds.), *Information Systems Security and Privacy* (Vol. 1221, pp. 335–357). Springer. https://doi.org/10.1007/978-3-030-49443-8_16

Ponsard, C., Grandclaudon, J., & Dallons, G. (2018). Towards a cyber security label for SMEs: A european perspective. *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, *2018-January*, 426–431. https://doi.org/10.5220/0006657604260431

Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine Learning Cybersecurity Adoption in Small and Medium Enterprises in Developed Countries. *Computers*, *10*(11), 150. https://doi.org/10.3390/computers10110150

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2021). Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME). *Future Internet*, *13*(8), 186. https://doi.org/10.3390/fi13080186

Riley, G. F., & Henderson, T. R. (2010). The ns-3 Network Simulator. In *Modeling and Tools for Network Simulation*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-12331-3_2

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2017.1476

Spruit, M. (2014). *ISFAM: The information security focus area maturity model OPERAM View project SMESEC View project*. https://www.researchgate.net/publication/288134391

Steele, S., & Wargo, C. (2007). An introduction to insider threat management. *Information Systems Security*, *16*(1), 23–33. https://doi.org/10.1080/10658980601051334

Stine, K., Quill, K., & Witte, G. (2014). *ITL BULLETIN FOR FEBRUARY 2014 FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY*.

UK Government. (2016). *Cyber Aware*. National Cyber Security Center.

Umam, S. (2020). Is the Cyber Security Awareness Perspective Different? *Journal of Business Management Review*, *1*(6), 425–435. https://doi.org/10.47153/jbmr16.772020

Urbach, N., Ahlemann, F., Böhmann, T., Drews, P., Brenner, W., Schaudel, F., & Schütte, R. (2019). The Impact of Digitalization on the IT Department. In *Business and Information Systems Engineering* (Vol. 61, Issue 1, pp. 123–131). Gabler Verlag. https://doi.org/10.1007/s12599-018-0570-0

van Haastrecht, M., Yigit Ozkan, B., Brinkhuis, M., & Spruit, M. (2021). Respite for SMEs: A Systematic Review of Socio-Technical Cybersecurity Metrics. *Applied Sciences*, *11*(15), 6909. https://doi.org/10.3390/app11156909

Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018). Simulations in cyber-security: A review of cognitive modeling of network attackers, defenders, and users. In *Frontiers in Psychology* (Vol. 9, Issue MAY). Frontiers Media S.A. https://doi.org/10.3389/fpsyg.2018.00691

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wiederhold, B. K. (2021). Increasing Cybersecurity Through Emotional Engagement. *Cyberpsychology, Behavior, and Social Networking*. https://doi.org/10.1089/cyber.2021.29224.editorial

Xinjie Chang. (1999). Network simulations with OPNET. *WSC'99. 1999 Winter Simulation Conference Proceedings. "Simulation - A Bridge to the Future" (Cat. No.99CH37038)*. https://doi.org/10.1109/WSC.1999.823089

Zúquete, A. (2021). *Segurança em Redes Informáticas* (6ª).