The Perceived Value of Cybersecurity Analyses and Frameworks for an IT Company

ELIAS BURKAN
ANDREI TANASE

SUPERVISOR

Jaziar Radianti

Marko Ilmari Niemimaa

University of Agder, 2021

Faculty of Social Sciences

Department of Information Systems

Preface

This thesis is written as a concluding assignment for the master's degree in Cybersecurity at the University of Agder in the Department of Information Science. It was conducted in the time period between January 2021 and June 2021.

The purpose this thesis had was to study how IT companies perceived the value of cybersecurity analyses and frameworks. Additionally, the aim was to help raise awareness for IT companies on which frameworks and cybersecurity analyses are suitable to improve the company's security.

First and foremost we would like to thank our supervisors, Associate Professor Jaziar Radianti and Associate Professor Marko Ilmari Niemimaa for their guidance and constructive feedback during the time period. Both supervisors have been easy to reach and available at all times, which has been both motivating and contributed to progress throughout the research. Additionally, we would like to thank the interview respondents that participated in this thesis, allocated their schedule, and shared their knowledge and insight with us. The data gathered from the interviews has been a paramount contribution and the respondents expressed a positive attitude with regards to us as researchers, which we greatly appreciated. Lastly, we would like to thank our friends and families for being supportive throughout this period.

Kristiansand

3rd June 2021

Andrei Tanase

Elias Burkan

Abstract

Recent trends show an increasing rate of cyberattacks against private companies and public organizations. Existing cybersecurity analyses and frameworks offer a set of guidelines for preparedness and security countermeasures against cyberthreats. However, there is little knowledge on the perceived value of these. This thesis explores the value of common cybersecurity analyses and frameworks, to understand their values for the organizations looking for a holistic overview of the possible countermeasures against cyberattacks. A choice made for the study was to mainly focus on IT companies as cases. To address the challenging nature of the thesis topic, three research questions were created. "*How does an IT company perceive the value of cybersecurity frameworks?",* "*What are the challenges of conducting a cybersecurity analysis?"* and *``How can performing a cybersecurity analysis benefit an IT company?".*

To answer these questions, the thesis incorporated a qualitative method, consisting of qualitative systematic literature review, semi structured interviews with IT companies of varying sizes and case studies. The *systematic literature review* formed a foundation for this thesis, especially to gain an understanding about the existing research regarding the selection of cybersecurity analyses. Some of the chosen ones are threat and risk analysis, penetration testing, and frameworks such as ISO 27000 series, OWASP and NIST. Additionally, the systematic literature review contributed to systematizing the presentation of the cybersecurity analyses and frameworks in a suitable manner. The literature review, accompanied by the interviews, provided new findings but also suggestions for future research. The *qualitative interview* was applied to obtain a holistic perspective and overview of how the IT companies manage and value their cybersecurity. *The exploratory case study* was used to analyze each company interviewed, in order to get an understanding of how each company sees cybersecurity and to dive deeper into their understanding and experiences in this field.

During the interviews, the respondents were asked to define the term value in relation to cybersecurity. Different companies require different security countermeasures, which is why size is one of the more important parameters. For a company to receive the most amount of value from a cybersecurity analysis or framework, they can be used in conjunction in order to supplement each other, so that a company can cover a wider area of concern. The case studies made it possible to explore the key characteristics, meanings and implications of the chosen case.

Based on the research, it is possible to conclude that all the companies interviewed would most likely benefit from the analyses or frameworks presented. Especially from free resources such as OWASP Top 10 list or flexible frameworks such as ISO and NIST. In addition, the analyses that are at the core of this thesis can help IT companies achieve a better overview over their assets, threats, risk and vulnerabilities. Furthermore, we concluded that in the domain of cybersecurity the term value is best described as the total monetary value of an asset that the organization deems important.

However, there are limitations to this study that are important to acknowledge. Two of these limitations are the amount of frameworks and analyses researched and the limitation regarding the number of interviews conducted. Since this is a particularly sensitive topic, it was difficult to get companies to talk about these topics.

In order for the research to have a broader view and provide more data, a suggestion would be to expand the study in both the quantity of countermeasures and the amount of interviews. This could lead to more accurate conclusions.

Table of contents

List of Tables

List of Figures

Chapter 1 - Introduction

In recent years there has been tremendous growth in cybercrime. A paper published by Statista (2020), which shows the total amount of cyber crimes in India has increased by 121% from 2016 to 2018 (Keelery, 2020). In actuality, several thousand attacks happen every day; Based on a report from Kaspersky Lab from 2016, a cyber attack occurs every 40 seconds (Kaspersky Lab, 2016, p.15). As a response to this type of crime, countermeasures have become more prevalent. There are an endless number of countermeasures, and some companies might feel overwhelmed by the options. Due to this, various companies may make a crucial mistake, which is what this thesis tries to preclude. In a study by Accenture Security they found out that nearly 70% of business leaders currently feel that their cybersecurity risks are increasing (Accenture Security, 2019). Additionally, this thesis aims to define the value of a handful of well known countermeasures. Despite the endless number of countermeasures, how organizations value countermeasures has not received sufficient attention. This thesis acknowledges the confusion surrounding these countermeasures, and ought to offer clarity.

The world is moving fast and technologies are ever changing, which may cause confusion for companies. The motivation behind this thesis was to study how different IT companies perceive the value of cybersecurity analyses and frameworks. Additionally, the aim is to help raise awareness for IT companies on which frameworks and cybersecurity analyses are suitable to improve the company's security. Despite the popularity and significance of cybersecurity, no research has assessed the perceived value of cybersecurity analyses and frameworks. The desired goal is to inform and help companies choose the correct method.

1.1 Key concepts

Value is a broad term used in multiple areas, such as economics, philosophy, principle of quality, historical value, etc. This thesis focuses on the cybersecurity aspect of value, which mainly includes economical aspects. This aspect can be narrowed down to privacy, cost of implementation versus anticipated cost of failure and loss of trust.

The term “countermeasures” is used by the authors as a collective name for cybersecurity analyses and frameworks. Companies might perceive the value of the countermeasures differently, therefore, value will be elucidated accurately. The reason companies might perceive the value differently is because there are multiple factors that play a role. The value might differ based on the size, goals or experience of the company. There are various ways to define cybersecurity analyses, evidently it is impossible for the scope of this thesis to include all available analyses. The chosen analyses that will be assessed and compared in this thesis are a threat analysis, a risk analysis, penetration testing, network and system monitoring, policies, and security awareness. Cybersecurity analyses are important, however it would be inadequate to exclude cybersecurity frameworks. Therefore, it is important to assess the value of these frameworks, especially when the aim is to create a holistic guide to cybersecurity. The frameworks to be included in this thesis are Open Web Application Security Project (OWASP), National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) 27000 family of standards. The analyses and frameworks were chosen as a result of their endorsement and reputation.

1.2 Research questions

Implementing cybersecurity analyses and frameworks is almost a necessity today. While keeping this in mind it is important to note that they are all different, and that there are multiple ones. This leads to several questions; Do we need them? Which ones do we choose? What are the benefits? Does one specific method require more time compared to others? These are important questions that need answers. Thus, the aims of this study are twofold. The theoretical background chapter, aims at clarifying and analyzing the use and need of a cybersecurity analysis and framework. Consequently, the research questions in this study will be created on the premise of the main topic.

"The perceived value of cybersecurity analyses and frameworks for an IT company"

This topic can be broken down into one main research question, with two sub questions that help answer the main question;

- **R1***: How does an IT company perceive the value of cybersecurity frameworks?*
- **R2***: What are the challenges of conducting a cybersecurity analysis?*
- **R3***: How can performing a cybersecurity analysis benefit an IT company?*

1.3 Research approach

The research approach utilized in this thesis was a combination of multiple research methods. The methods included were a systematic literature review (SLR) and semi structured interviews (SSI) which founded the four case studies. These qualitative methods were all chosen through research and aided to create the thesis structure. The research methods provided the theoretical foundation and findings so that it was possible to answer the research questions.

1.4 Thesis structure

The thesis is organized into eight chapters. The first chapter introduced the problem statement and research questions, along with why this is an important subject to research. The second and third chapter presents the analyses and frameworks, which is the theoretical background for this thesis. The fourth chapter explains the research approach of the thesis. The fifth chapter presents the research profile of the respondents from the qualitative interviews. The sixth chapter presents the findings, whilst the seventh chapter discusses the literature review and interviews. The last chapter is the conclusion, where the most important findings and a summary is presented.

Chapter 2 - Cybersecurity analyses

This chapter introduces the cybersecurity analyses which are part of the foundation of the thesis. The information gathered creates the foundation for this chapter and is a result of conducting a systematic literature review. The process of conducting an SLR is described in further detail in chapter *Research approach*. These concepts are relevant theories to enlighten the research questions mentioned in the introduction. First and foremost, it is important to create a fundamental understanding of what cybersecurity analyses are. Following, each analysis will be described in detail and the reason for choosing those specifically will be justified. Lastly, this chapter explains the importance of these countermeasures.

For the purposes of this thesis, cybersecurity analyses will be used as an umbrella term for the different methods that will be presented in the following subchapters. The term cybersecurity analyses encapsulates different methods that can be used in order to assess and analyse any cybersecurity related threats, vulnerabilities and risks. It is therefore important to understand how this term will be used in the thesis before continuing with the introductions of each method. The common denominator between these analyses is that they all have the same goal, which is to enlighten the users on their current cybersecurity situation. The umbrella term "analyses" in this thesis, ranges from theoretical concepts to more technical and practical countermeasures. The analyses are beneficial because they provide cybersecurity professionals with a greater understanding of their security needs.

The cybersecurity analyses that have been chosen are some of the most well known and widely used security analysis methods. One advantage surrounding these methods is that since they are widely used there is a lot of information on how to best make use of them. Thus making it more approachable for cybersecurity professionals to implement them in their own IT system.

2.1 Threat analysis

Threat analysis is a process used to determine which components of a system need to be protected and what type of threats they should be protected from (McCabe, 2007, p. 363). The information that is gathered through performing a threat analysis can be used by organizations to better determine key locations in the system where security can be improved. As mentioned, a threat analysis typically consists of finding different assets that should be protected, but also identifying and evaluating the possible threats related to the assets. According to McCabe, assets can include:

- Workstations/PCs
- Servers
- Network devices (switches, router, AP)
- Software
- Data

While some potential threats can include:

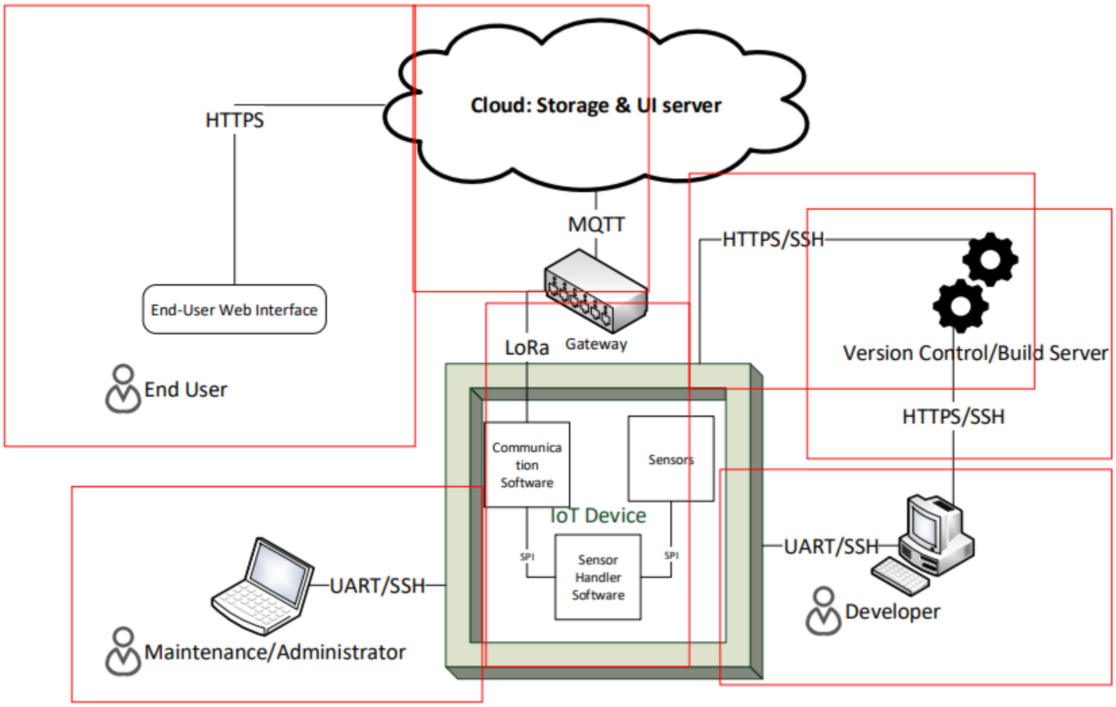
- Unauthorized access to data/services/software/hardware
- Denial of service
- Theft of data/services/software
- Unauthorized disclosure of information
- Viruses, worms, trojan horses

McCabe also discusses that threat analyses are subjective by nature. This is because the results of the threat analyses will be influenced by the persons doing the analysis. He therefore proposes that in order to minimize the degree of subjectivity, one should aim to involve representatives from different parts of the organization. This would ensure that the threat analysis has a holistic approach. Furthermore, McCabe also notes that since organizations grow and change over time, it is important that threat analyses are conducted periodically. Thus ensuring that new potential threats are discovered in time and the organization has a chance to implement new security mechanisms (McCabe, 2007, p. 364).

A method of using threat analysis in a development cycle can be threat modeling. Threat modeling is a process where the developers of a device or system consider potential scenarios where the device or system is at risk (Nummikallio, 2019, p. 5).

Figure 1

Diagram of a system using trust borders



Copied from “ Internet of Things Devices: Case Studies on Security” by A. Nummikallio, 2019, p. 6

As seen in Figure [1], threat modeling begins with categorizing each component of a system. This is done in order to find out how the system is set up and to identify potential weak points in the architecture. The developers also identify where data is being transferred between the different components. The transfer points are marked with red borders in the figure, also called trust boundaries. Once the information flow and the system components have been defined, it is easier to also imagine and categorize which threats are related to the devices (Nummikallio, 2019, p. 6). Any organization can in theory use a threat analysis. The threat analysis must not cover every single aspect of the organization, but it will help to get a more clear understanding of potential threats that can harm the organization's assets and information. The value of the threat analysis method is related to the high level of flexibility it has, but also to the amount of information that the analysis helps uncover.

Threat analysis can help a security team to stay on top of the evolving threats across their platform, and ensure that necessary protections are in place. Additionally, it can reduce the attack surface, which refers to the total number of vulnerabilities that an organization or company is exposed to. Another benefit with threat analysis is that it helps recognize and prioritize which threats to focus on, especially because of the economical restrictions an organization might have. Threat analysis also identifies and eliminates single points of failure, which means that through conducting a threat analysis it encourages organizations to use layers of defensive tools to protect their valuable assets. This reduces the chance for a threat actor to find a vulnerability in a single point of failure in a system (Mallory, 2020).

2.2 Risk Analysis

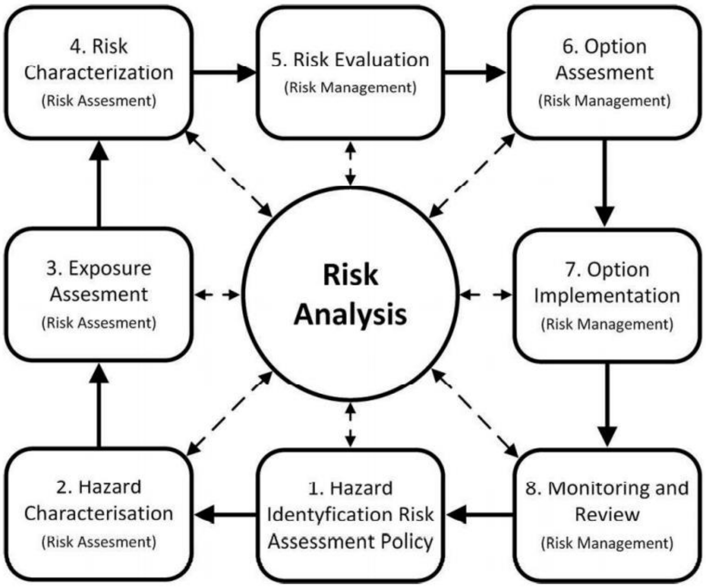
The concept of risk analysis is not something new, it is an age old concept that has been around for more than 2400 years. It is known that the Athenians offered their capacity of assessing risk before making decisions (Aven, 2016). However, the concept is young in the scientific field and in the last 30 to 40 years, it has been emerging in scientific journals, papers and conferences. All of the aforementioned documents try to appropriately apply the principles of risk analysis. Since then the field has been considerably developed with new and more sophisticated analysis methods and techniques (Aven, 2016). In this subchapter, risk analysis will be analyzed; why we need it and what it is, followed by practical examples.

In relation to cybersecurity, cyber risks are associated with events that could potentially result in a data breach. Cyber risks are not to be confused with vulnerabilities, as vulnerabilities are weaknesses that result in unauthorized access if exploited, and cyber risks are the probability of a vulnerability being exploited (Tunggal, 2021).

Risk analysis can imply examining how project outcomes or objectives might change due to the impact of a risk event. As soon as the risks are identified they are analyzed to identify either the qualitative or quantitative impact the risk might have on the project. Once that is accomplished it becomes more straightforward to take the appropriate steps to mitigate said risks (Lavanya & Malarvizhi, 2008). In a study by Czechowski (2016), he discusses the overall process and issues regarding risk analysis and assessment of threat probability regarding cybersecurity in electrical power systems. Although this thesis does not focus on electrical power systems, there is still relevant information that can be extracted from Czechowski's article. Prior to conducting his analysis, Czechowski states just how important these electrical power systems are and that nearly all systems are dependent on the supply of electricity (Czechowski, 2016, p. 23).

Figure 2

Risk analysis diagram process

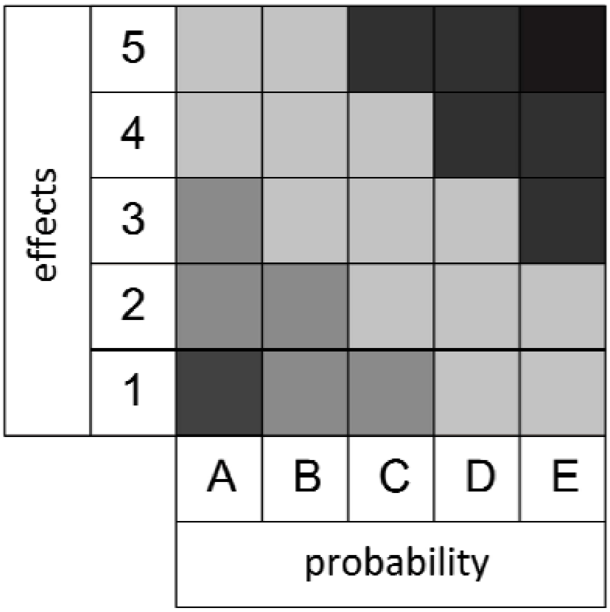

4. Risk Characterization (Risk Assesment)
5. Risk Evaluation (Risk Management)
6. Option Assesment (Risk Management)
3. Exposure Assesment (Risk Assesment)
Risk Analysis
7. Option Implementation (Risk Management)
2. Hazard Characterisation (Risk Assesment)
1. Hazard Identyfication Risk Assessment Policy
8. Monitoring and Review (Risk Management)

Copied from "Cybersecurity Risk Analysis and Threat Assessment Within Smart Electrical Power Distribution Grids" by R. Czechowski, 2016

The analysis procedure can be written, graphical or tabular, based on the given situation. According to Czechowski, it is also recommended to include a map indicating the area and reach of a potential threat separately for each scenario. It should include all important information that may have an impact on the final assessment. Czechowski states that a detailed risk analysis should be divided into individual analytical decision-making and implementation stages. Once the probability and consequences of the risk have been determined, it is possible to indicate the risk value. Risk values are indicated on the risk matrix, which shows the dependence between probability and consequences, as shown in Figure [3].

Figure 3

Risk analysis table.



Copied from "Cybersecurity Risk Analysis and Threat Assessment Within Smart Electrical Power Distribution Grids by R. Czechowski, 2016

The visualization helps with quick classification of the given event, additionally it allows for reading the distribution of most critical situations in relation to their probability. Czechowski ends the chapter by saying that the risk analysis estimation is a complicated process. The process requires a vast amount of knowledge of its creation methodology as well as practical knowledge of the industry (Czechowski, 2016, p. 24-25). The value a risk analysis can bring to a company is completely dependent on the situation, if it is applicable or even if it is the right time to conduct one. Risk analysis goes way beyond only the technical risks; it ranges from the human aspect to natural events such as natural disasters or diseases. That being said, the value of being aware of risks comes from gaining knowledge on where to focus the attention.

2.3 Penetration testing

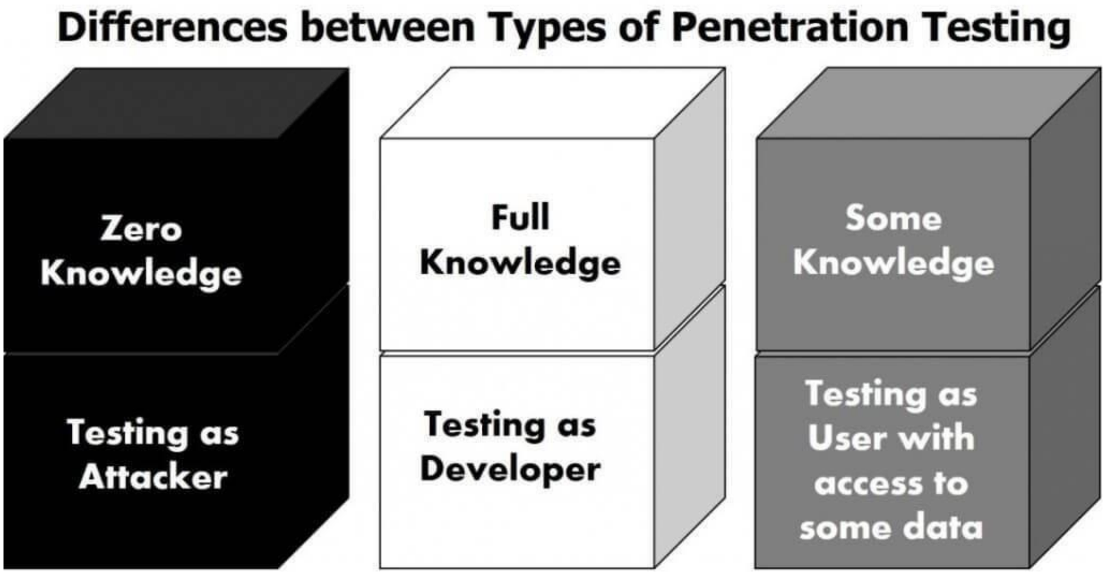
Penetration testing is an extensive process or method to test the complete integrated, operational and trusted computing base that contains hardware, software and people (Bacudio et al., 2011, p. 19). The process requires an active analysis of the system to find any potential vulnerabilities. This includes poor or improper system configurations, hardware and software flaws and operational weakness in the process or technical countermeasures. Penetration tests are useful tools to discover and address vulnerabilities in a network's infrastructure, showing how vulnerable to malicious attacks some networks really are. It is common for an attacker to exploit and penetrate a victim’s system without them consenting or even knowing about the attack (Stiawan et al., 2017, p. 126). This could be used as a security measure if the organization has planned this in advance. For this reason penetration testing works as a security analysis approach in relation to this thesis’s key concepts.

There are three common penetration strategies: black, grey and white box, as seen in Figure [4].

In a black box environment the penetration tester represents a hacker from the outside with no prior knowledge of their internal systems. In a grey box environment the hacker has access and potentially knowledge of a user with some elevated privileges. They usually have some knowledge of the network internals and some architecture documentation. The grey box testers are usually more focused and know which areas they want to test, instead of determining this themselves. White box hackers are the opposite of black box hackers and are given full access to the source code, architecture documentation, etc. It is the most time consuming type of testing, as one needs to learn a great amount of information to identify potential points of weakness.

Figure 4

Black, white and grey box penetration testing


Differences between Types of Penetration Testing
Zero Knowledge
Testing as Attacker
Full Knowledge
Testing as Developer
Some Knowledge
Testing as User with access to some data

Copied from "Black Box vs. White Box Testing: Key Differences Every organization Should Know" by CoreSentinel, n.d

2.3.1 Penetration testing types. There are several ways to conduct a penetration test, but the most common ones are network tests, application tests and social engineering. Network penetration testing is an ethical and safe course of action to identify security gaps or flaws in the organization's network. The penetration testers perform analyses and exploits to evaluate whether their equipment can be used to gain unauthenticated access. Application penetration testing is an attack simulation which is intended to expose application security controls by utilizing risks created by real exploitable vulnerabilities (Bacudio et al., 2011, p. 21). Although organizations or companies have firewalls and monitoring systems set up to protect information, their security may still be vulnerable since traffic is allowed to pass through their firewalls.

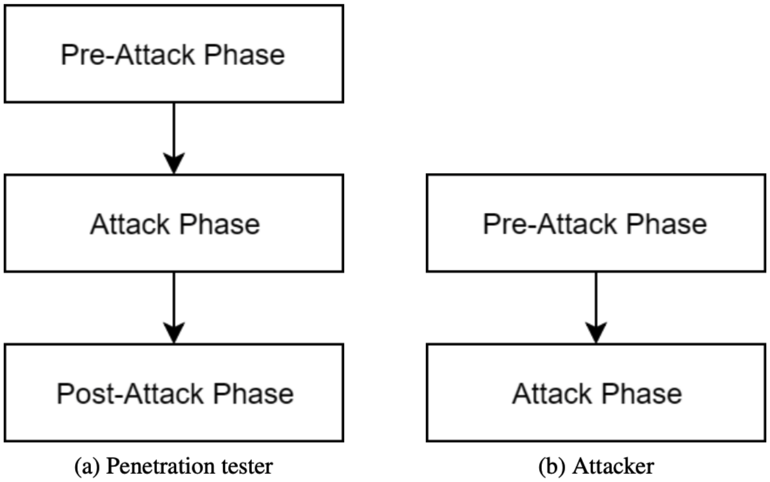
Social engineering exploits human interaction to obtain or compromise information about a computer system or an organization. It is used to discover the level of security awareness among the employees in the organization that maintains the target system. This is useful to test the ability of the organization to prevent unauthorized access to their information systems (Bacudio et al., 2011, p. 22). In a study by Jalkanen Jaakko (2019), an in-depth literature review is conducted to find out if humans are the weakest link in information security. According to him, the research topic proved to be complex and not straightforward, although the majority of the studies he included in his literature review implied that humans were the weakest link (Jalkanen, 2019, p. 49).

2.3.2 Penetration testing in practice. In a study by Filipe Pestana Duarte Rocha (2019), various means are used to analyze a Supervisory Control And Data Acquisition (SCADA) system, including a penetration test. During the study, grey box penetration testing is conducted in a lab environment to not crash the actual systems, as they require 100% uptime, and these scans may cause the systems to crash. They did three types of penetration tests, reconnaissance, vulnerability mapping and exploit known vulnerabilities (Rocha, 2019, p. 79).

Reconnaissance is the act of collecting useful information about a target, and their devices that the network contains. It is usually the process before the attacking part happens, as illustrated in Figure [5].

Figure 5

Cyber attack phases.



(a) Penetration tester

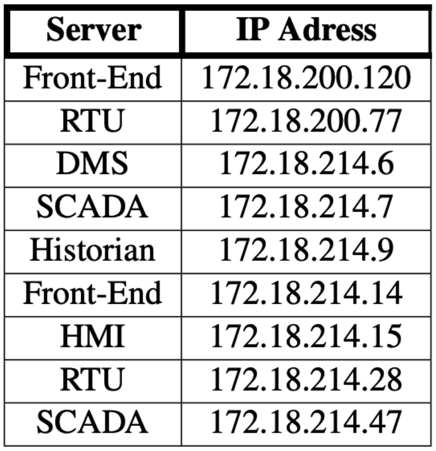
(b) Attacker

Copied from “Cybersecurity analysis of a SCADA system under current standards, client requisites, and penetration testing” by F.P.D. Rocha, 2019

This section will only focus on the reconnaissance of the study, where an active scanner and a passive scanner were used. Their active scanner was NMAP, which is a free and open source utility for network discovery and security auditing. NMAP uses raw IP packets in novel ways to find what hosts are available on the network, and what services these hosts offer, what operating systems they are running, etc.(NMAP n.d). The port scan discovers which ports are on the targeted device and enumerates the services that are running on each of these ports. This is done so that the tester can discover which applications provide the service, the applications versions and what operating system the device is running. In the Figure [6], it is displayed what type of information was gathered through port scanning in the SCADA system.

Figure 6

Important hosts on the network



Server	IP Adress
Front-End	172.18.200.120
RTU	172.18.200.77
DMS	172.18.214.6
SCADA	172.18.214.7
Historian	172.18.214.9
Front-End	172.18.214.14
HMI	172.18.214.15
RTU	172.18.214.28
SCADA	172.18.214.47

Copied from “Cybersecurity analysis of a SCADA system under current standards, client requisites, and penetration testing” by F.P.D. Rocha, 2019

There were however some considerations to take when the tester port scanned, as the system was quite fragile and prone to poor performance (Rocha, 2019, p. 78-81). Through reconnaissance or other types of penetration testing tools it is possible to map out vulnerabilities in a system, similar to other analyses such as risk analysis or threat analysis. If a company is worried about attackers, it is a viable strategy to hire black, grey or white penetration testers to find its own vulnerabilities before anyone with malicious intent does.

2.4 Network and system monitoring

Network and system monitoring are closely related, but they monitor different aspects of a company. Network monitoring is an important part of network management, and has been widely used in intrusion monitoring and protocol analysis. Network monitoring has several benefits, and can solve vulnerabilities in system software, errors and other security related issues to protect the network security (Lv et al., 2018, p. 27). System monitoring or IT monitoring has evolved drastically to keep up with the complexities of modern IT environments. IT monitoring tools can monitor on premises or cloud based systems. The concepts inherent to IT monitoring have a crossover with other disciplines, including Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR) and more (Splunk, n.d).

2.4.1 Network monitoring. Network monitoring provides necessary information on a network that the administrators use to determine if the network runs optimally. Using network monitoring tools, administrators can, among other things, proactively identify deficiencies and optimize efficacy of the network. Network monitoring systems include software and hardware tools that can get information on various aspects of a network, such as the traffic, bandwidth, utilization and uptime. They may also detect devices and other elements that touch the network, and will provide status updates on the network (Cisco, n.d). A type a threat that network monitoring can help detect is called distributed denial of service (DDOS). DDOS attacks atempts to overwhelm websites and online services with more network traffic than the servers or infrastructure can accommodate (Weisman, 2020).

2.4.2 System monitoring. System monitoring is a fundamental component of an IT team’s responsibilities. While frameworks like NIST offer guidelines for monitoring, the standards can leave room for interpretation. There are several types of data which are important to monitor. Perhaps the most important one is log data, which can be defined as data written to a log file independently of whether it has a common structure or a simple text file. Another data type which is important is the asset data, which refers to any data taken directly from an asset.

This ranges from resource metrics like CPU and memory to information about processes and applications (Rapid7, n.d).

A common and widely used application for system monitoring is Splunk. Splunk is a SIEM tool which offers a variety of unique tools. It is a software you can give machine data and Splunk will process the data for the user. An area Splunk often is used in is log management, it offers to quickly and easily search through all log files. The users may also make simple code changes so that the readability of these logs improve, as there can be a lot of data and can be confusing to read. Logs can be a hassle to deal with; they don't have structure, the users can be clueless about where the logs came from and it can be overwhelming because of the sheer amount of information. On the other hand, logs are really useful as they contain a large amount of valuable analytic information and can tell the user about problems that happened so that the organization can resolve a problem before it happens again. The logs provide information about the IT infrastructure, behavior of users and can identify potential attackers (Splunk, n.d).

2.5 Policies and security awareness

Policies and security awareness controls might be one of the most important aspects when trying to uphold good information security inside a company. Before explaining what policies and security awareness are, it must be clear why the human aspect of an organization poses the highest threat. The common denominator for all activities and vulnerabilities that are related to the human aspect of an organization is called the human attack surface. Some types of vulnerabilities and risks that are considered part of the human attack surface include negligence, human errors, illness, death, inside threat and the susceptibility to social engineering (Wigmore, Ivy, 2017). Humans have a curious nature, and for that reason people tend to click on links they receive via email. When this is done without any further thought, it can lead to a security breach. Increasing the level of security awareness can therefore be done through training and by implementing policies.

2.5.1 Policies. Policies serve as rules that employees of a business have to adhere to when working within the company's IT system. A paper by Höne & Eloff (2002), describes what makes an effective information security policy. They note that it is important to create the policy in such a way that users can identify when the policy applies, but must also be clear enough so that the users know how they should manage information resources (Höne & Eloff, 2002). In another study by Höne & Eloff, they note that information security policy is one of the most important documents in an organization. Due to this, it is crucial that the person responsible for writing the policy uses different international standards. This is done in order to make sure the basic security areas are covered by the security policy (Höne & Eloff, 2002).

It is important that an organization has policies in place, and by using different standards, these policies can be created in such a way that they make sense and are easily understood. The value of policies is dependent on the effectiveness of the policy in question. If a policy is easily understood, it may offer a higher value when trying to combat security risks than a policy that is intrusive or limiting by any way. Moreover, policies can be a free or bought service depending on the current security knowledge on the IT personnel.

2.5.2 Security awareness. Alongside policies, the security awareness of users working with IT systems is important. This is because of the human attack surface mentioned earlier. Training employees how to think and react to potential security attacks is necessary in order to create a holistically secure system (Grassegger & Nedbal, 2021). It is important to keep in mind that humans are still susceptible to social engineering attacks. With that being said, one of the most common forms of social engineering that exploits the human attack surface is phishing. An example of phishing is the fraudulent practice of sending emails that seem to come from a trustworthy source in order for the receiver to reveal personal information, such as login credentials or financial information (Cuchta et al., 2019, p. 1). In a business environment, phishing attacks can lead to information disclosure, ransomware infiltration or theft of login credentials.

A study by Cuchta et al. (2019), proposes to find out which different methods of raising security awareness can help mitigate against successful phishing attacks. The study begins with the authors sending out common phishing emails to a large number of users at a university and after presenting different methods to raise security awareness for the test group (Cuchta et al., 2019, p. 3). The authors propose three different methods: long text-based documents, visual-based documents and an interactive game. After conducting the experiment they were able to conclude that the visual-based documents and the interactive methods worked best to raise the security awareness of the test subjects (Cuchta et al., 2019, p. 5). The goal was to minimize the risks surrounding the human attack surface as this is one of the most prevalent breaching points for an organization's IT system.

Another way of increasing security awareness inside a company besides the aforementioned methods, can be through establishing a good security culture. Usually culture in an organization means “the way things are done here” and it can be seen as the personality of the company. In a study by Da Veiga and Eloff (2010), they present security culture as the attitudes, assumptions, beliefs, values and knowledge that employees use to interact with the organization’s systems and procedures at any point in time. The interaction results in acceptable or unacceptable behavior evident in artifacts and creations that become part of the way things are done in the organization to protect its information assets (Da Veiga & Eloff, 2010).

Security culture might be the best way to increase and improve the total security of an organization. If employees are trained and have good security awareness over time, this can lead to developing a security culture. The value of good security policies, awareness and culture, is that it helps reduce the risks related to the human attack surface. An established security culture inside an organization will promote good security without necessarily requiring continuous monetary investment. With that being said, security culture is not always the perfect solution. Security culture cannot be implemented without being backed up by good technical security and individual security awareness. It is only when the whole IT system is holistically secure that good security culture can help achieve the last percentage towards better security.

Chapter 3 - Cybersecurity frameworks

This chapter will explain the chosen frameworks and give an introduction on how they work. This will give the reader an easier time understanding the value of these cybersecurity frameworks. Before we dive into the specifics regarding these frameworks, it is important to know what they are and how they are useful. The focus will be on three different frameworks: OWASP, ISO and NIST, these are all well known cybersecurity frameworks that are commonly used at this moment in time.

Cybersecurity frameworks provide standards and guidelines to secure a company or organization against cyber adversaries. They are commonly used to secure their organization and ensure compliance with the mandates in a framework. The frameworks provide guidance for improving a cyber risk program. The advantage of utilizing a framework is that it gives consistency across different functions and shows a uniform set of goals. Some frameworks offer guidance on where to begin when securing your organization from the most common cyberthreats, while others provide best practices and processes that help the foundation of a risk reduction plan (Axio, 2020). When a framework is applied correctly, it may enable an organization's IT security leaders to manage cyber risk more rationally compared to others who do not use a framework. Some organizations must comply with required government regulations for them to be allowed to operate. For example, a company that handles credit card transitions must prove that it complies with the popular Payment Card Industry Data Security Standards Framework (Garcia, 2019).

3.1 OWASP

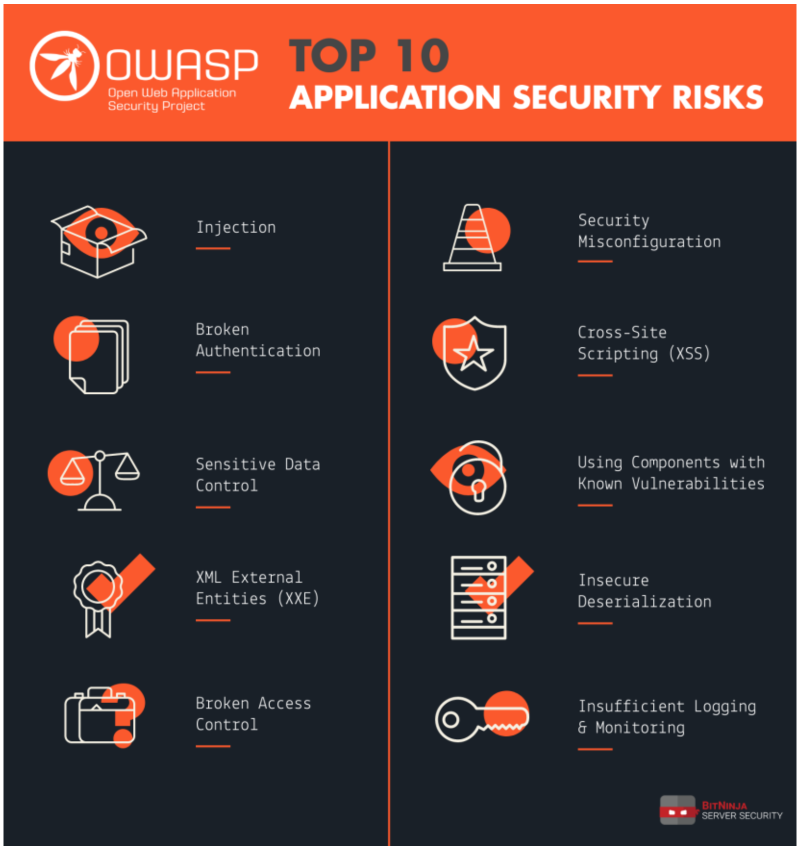
The following sub-chapter presents OWASP Top 10. OWASP stands for Open Web Application Security Project, and is a non-profit organization that has been started with the goal to help improve the security of software. The OWASP Top 10 list was created by the OWASP Foundation and is meant to serve as a standard awareness document and guidelines for developers of web applications. The list presents the Top 10 most common flaws and security risks that a web application can be vulnerable to. The guidelines are meant to be applied throughout the development lifecycle of an application. This is recommended in order to avoid any potential vulnerabilities at any of the development stages: system planning, system analysis, system design, implementation and testing (Arya Wiradarma & Arya Sasmita, 2019). It is important for a developer to be aware of these different risks as web applications are commonly targeted by malicious attacks.

Based on a community survey that OWASP conducted in 2020, it is shown that the majority of respondents of the survey were mostly satisfied with OWASP. Noting that the quality and availability of information online is something that is greatly appreciated by the OWASP community. The survey also notes that the respondents who use OWASP in their projects also find it mostly useful (OWASP, 2020). Again, this is related to the content that OWASP provides to its community, as well as the large number of members that can rely on each other in case they have some questions related to security practices.

For the purpose of this thesis we will not explain all of the vulnerabilities from the OWASP Top 10 list in detail. We will mainly focus on giving a broad explanation on why the vulnerabilities and risks presented in the Top 10 list are important and should be handled with care. All the risks and vulnerabilities are presented in order in Figure [7]. More information about the OWASP Top 10 list can also be found on the OWASP website (OWASP, 2017).

Figure 7

OWASP Top 10 List


OWASP
Open Web Application Security Project
TOP 10
APPLICATION SECURITY RISKS
Injection
Broken Authentication
Sensitive Data Control
XML External Entities (XXE)
Broken Access Control
Security Misconfiguration
Cross-Site Scripting (XSS)
Using Components with Known Vulnerabilities
Insecure Deserialization
Insufficient Logging & Monitoring
BitNinja SERVER SECURITY

Copied from "Web Application Firewalls: Choosing the right WAF for server security" by A. Batari, 2017

Most of the risks and vulnerabilities in the list are related to the development and implementation of a web application. They pose an ever growing threat to web applications and software in general. As more commodities are digitized, we see an increase in cyber attacks that try to utilize these known vulnerabilities. Some examples of cyber attacks are: injection attacks, attacks that try to exploit weak authentication and attacks that target known vulnerabilities in software and hardware. The goal that OWASP has, was to categorize the vulnerabilities and potential exploits in order for anyone to know which steps to take for their web application to be as safe as possible.

3.1.1 Advantages of using OWASP. The advantages of adopting OWASP are mostly related to how an organization is capable of handling vulnerabilities and what measures need to be taken in order to improve overall application security (Mylonas, 2020). Since OWASP mainly was created as guidelines and best practice tips related to application development, most of the security measures they propose might only apply to organizations that develop applications. With this being said, since almost all organizations have an online presence today, they are not excluded from the risks and vulnerabilities that OWASP tries to shine a light on. Furthermore, the OWASP list and documentations are a free resource, which means that they are available for anyone to use and implement as they please. Some of the vulnerabilities presented in the Top 10 list may not even apply for some businesses, but because the OWASP list is a free resource, it is beneficial to be aware of it. The resources are available to help developers, business owners and IT professionals learn from the mistakes of others while giving them guidance on how to better mitigate the risks and vulnerabilities related to the list (Groski, 2013). In addition, an important aspect of OWASP is that it is an ongoing project and it has a large community. This means that the guidelines and vulnerabilities presented are always kept up-to-date and relevant for IT professionals to rely on. Compared to other standards and frameworks that cost money, a large advantage of the Top 10 list is that it is a free resource.

3.1.2 Use case of OWASP Top 10. In a study by Sechel (2017), he uses the OWASP Top 10 list together with the OWASP Risk Rating Methodology in order to analyze systems that can potentially be vulnerable to one or more items from the OWASP list. In his paper, Sechel shows that the OWASP Risk Rating Methodology builds upon the OWASP Top 10 list and can be used as an analysis method to identify and categorize both technical and business risks. The methodology takes into consideration that any vulnerable part of the system can impact the organization in both technical and business aspects (Sechel, 2017, p. 18).

3.2 ISO standards

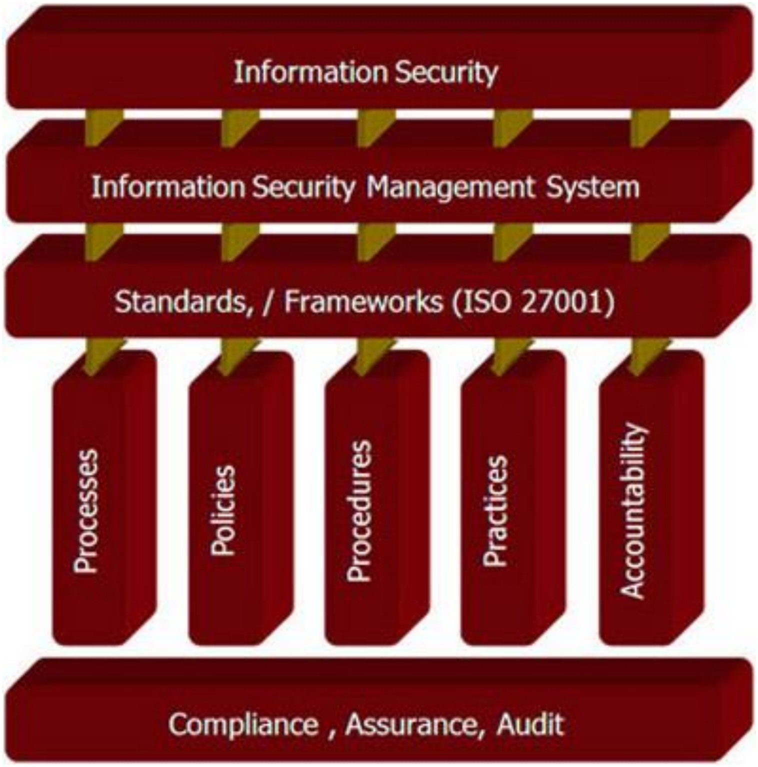
ISO was founded in 1947 as a standard-setting organization, and is composed of 165 non-governmental organizations from different countries. ISO produces and manages international standards for almost all the aspects of industries and technologies, not only cybersecurity. The main purpose of ISO is to create standards that help build reliable, safe and quality products, systems and services that can be used worldwide. As of 2018, ISO had published over 20 000

International Standards (Renvall, 2018, p. 38). Norway has a national member of ISO called Standards Norway (SN).

3.2.1 What is the ISO 27000-series? For the purposes of this study, we have chosen to look at the ISO 27000-series and mainly the ISO 27001 standard. This family of standards focuses on providing best practices and recommendations on how to manage information security in an organization (ISO, 2013). The 27000-series of standards was first introduced in the late 1980's, but has since been revised a couple of times. The latest edition of the ISO 27001 standard was published in 2013. The goal of the standard is to offer guidance so that companies are able to better decide which cybersecurity solutions best cover their needs. It is not a ready made list of specific technical solutions that organizations need to implement (Renvall, 2018, p. 38).

Figure 8

ISO Structure


Information Security
Information Security Management System
Standards, / Frameworks (ISO 27001)
Processes
Policies
Procedures
Practices
Accountability
Compliance , Assurance, Audit

Copied from "Lecture-1-Introduction-to-Security-Management" by S.H. Othman , 2017

The ISO 27001 standard consists of ten clauses and an Annex A. The clauses and annex are the foundation of the standard, and it is recommended that any organization who wants to implement an information security management system (ISMS) strongly follows these steps. The clauses are as follows.

Table 1

Structure of the standard

0 Introduction	The standard describes a process for systematically managing information risks
1 Scope	It specifies generic ISMS requirements suitable for organizations for any type, size or nature
2 Normative references	Only ISO/IEC 27000 is considered absolutely essential to users of ISO 27001
3 Terms and definitions	See ISO/IEC 27000
4 Context of the organization	Understanding the organizational context, the needs and expectations of "interested parties" and defining the scope of the ISMS
5 Leadership	Top management must demonstrate leadership and commitment to the ISMS, mandate policy, and assign information security roles, responsibilities and authorities
6 Planning	Outlines the process to identify, analyze and plan to treat information risks, and clarify the objectives of information security

7 Support	Adequate, competent resources must be assigned, awareness raised, documentations prepared and controlled
8 Operation	A bit more detail about assessing and treating information risks, managing changes, and documenting things (partly so that they can be audited by the certification auditors)
9 Performance evaluation	Monitor, measure, analyze and evaluate/audit/review the information security controls, processes and management system, systematically improving things where necessary
10 Improvement	Address the finding of audits and reviews (e.g. nonconformities and corrective actions), make continual refinements to the ISMS

Copied from "Information security management systems - Requirements" by ISO, 2013

As mentioned above, in addition to the clauses, ISO 27001 also includes a comprehensive list of security controls and objectives that is called Annex A. The Annex consists of a further 14 clauses which include 114 security controls grouped up into 35 control categories. An important thing to note is that in the newest version of ISO 27001:2013, the security controls are no longer a requirement for organizations to use. The standard has become more flexible and allows companies to choose and implement only the controls that are suitable for their own needs. In the following list the main 14 topics of the ISO 27001 Annex A are presented.

Table 2

ISO 27001 Annex A

A.5 Information security policies	Controls on how the policies are written and reviewed
A.6 Organization of information security	Controls on how the responsibilities are assigned, also includes the controls for mobile devices and teleworking
A.7 Human resources security	Controls prior to employment, during and after the employment
A.8 Asset management	Controls related to inventory of assets and acceptable use, also for information classification and media handling
A.9 Access control	Controls for the management of access rights of users, systems and applications, and for the management of user responsibilities
A.10 Cryptography	Controls related to encryption and key management
A.11 Physical and environmental security	Controls defining secure areas, entry controls, protection against threats, equipment security, secure disposal, Clear Desk and Clear Screen Policy, etc
A.12 Operational security	Lots of controls related to the management of IT production: change management, capacity management, backup, logging, monitoring, installation, vulnerabilities, etc
A.13 Communications security	Controls related to network security,

	segregation, network services, transfer of information, messaging, etc
A.14 System acquisition, development and maintenance	Controls defining security requirements, and security in development and support processes
A.15 Supplier relationships	Controls on what to include in agreements, and how to monitor the suppliers
A.16 Information security incident management	Controls for reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence
A.17 Information security aspects of business continuity management	Controls requiring the planning of business continuity, procedures, verification and reviewing, and IT redundancy
A.18 Compliance	Controls requiring the identification of applicable laws and regulations, intellectual property protection, personal data protection, and reviews of information security

Copied from “A quick guide to ISO 27001 controls from Annex A” by Leal, n.d

However, Annex A is designed to be used together with the ISO 27002 standard. This is because the clauses from ISO 27002 are the same as the ones in Annex A. The only difference being that in ISO 27002 the clauses are described in more detail (Renvall, 2018, p. 41).

3.2.2 Advantages with ISO. It is important to know where the ISO 27000-series and especially ISO 27001 can be best utilized. In a study by Aleksi Renvall (2018), he notes how the flexibility and versatility of the ISO 27000-series can help small and medium size enterprises meet their security goals without incurring significant financial expenses. He specifies that smaller businesses can purchase guidelines so that the implementation of the ISO security measures is less of a hassle. Additionally the ISO standard is so versatile that businesses do not need to implement all of the security controls in order to get ISO certified; companies can choose which ones they need and call themselves ISO compliant (Renvall, 2018, p. 47).

One of the largest advantages of the ISO standard is its global recognition. If a business is ISO certified or compliant it may increase the businesses reputation, which can potentially be of great value for the company.

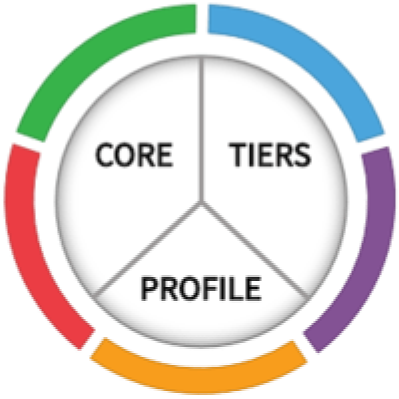
3.3 NIST

The National Institute of Standards and Technology (NIST) was founded in 1901 and is not just related to cybersecurity. From smart electric power grids and electronic health records to atomic clocks, advanced nanomaterials and computer chips, these services rely on technology, measurement and standards provided by NIST (NIST, 2017). Originally NIST was named “Bureau of Standards”, and their goal was to ensure a consistent standard of size and function as laboratory standards. NIST was used extensively in the cybersecurity sector in 1967 (Krumay et al., 2018, p. 226). During this chapter however, the focus will solely be on their flexible and dynamic cybersecurity framework. In February 2013, the president of the USA issued the executive order to improve the cybersecurity of critical infrastructure, which led to NIST working with stakeholders to develop a voluntary framework based on current standards, guidelines and practices. The framework attempts to help organizations manage and reduce risks, it was developed and designed to foster risk and cybersecurity management communications amongst stakeholders. The cybersecurity framework’s first version was publicly accessible in 2014 and updated to version 1.1 in 2018 (Krumay et al., 2018). According to Krumay et al., NIST cybersecurity framework components are more appropriate for technology organizations to use as their scope for technical control, log analysis, and incidents (Krumay et al., 2018, p. 226).

The framework consists of three main components: the core, implementation tiers, and profiles as seen in Figure [9]. The concept of the framework is to provide cybersecurity activities and outcomes using common language understandable to a layman. The core part of the framework guides organizations in managing and reducing their cybersecurity risk in a way that compliments their current measures. The implementation tiers section assists organizations by providing context on how organizations view their cybersecurity risk management. The section guides organizations to an appropriate level of thoroughness for their cybersecurity program, which commonly is used as a tool to discuss risk appetite, mission priority and budget. The last segment of the framework is the profile, which is an organization's unique alignment of their requirements and objectives, risk appetite and resources compared to their desired outcomes of the framework core. Most commonly profiles are used to identify and prioritize opportunities for enhancing cybersecurity at the organization (NIST, 2020).

Figure 9

NIST framework components

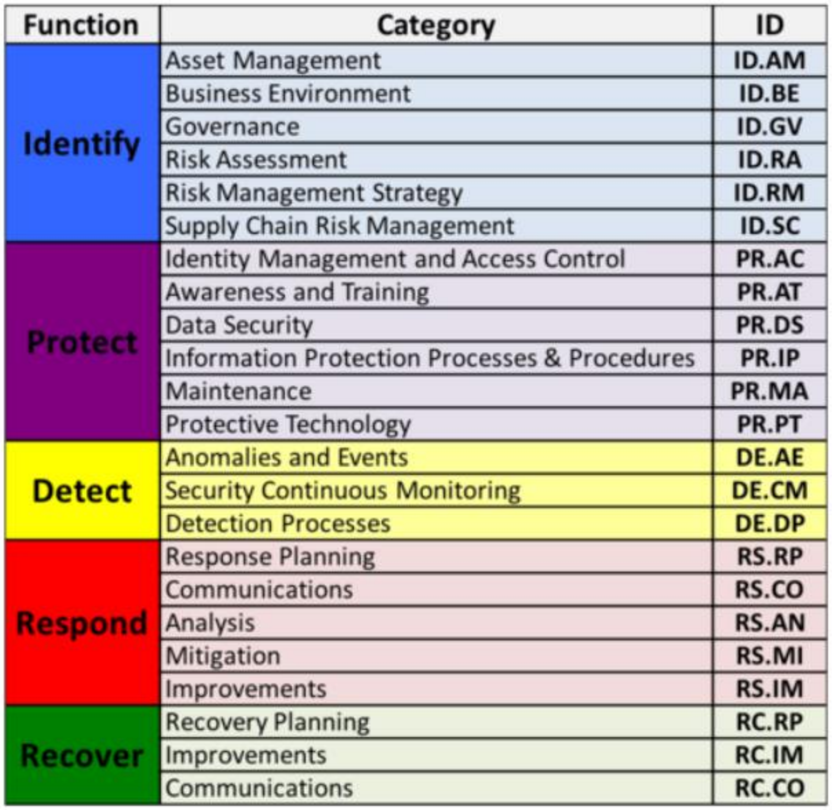


Copied from “An Introduction to the Components of the Framework” by NIST, 2020

3.3.1 Framework core. The core is a set of sought-after cybersecurity activities and end results organized into several categories and aligned to informative references. The framework core is designed to be intuitive for everyone, and to function as a translation layer in order to enable communication between technical and non-technical teams. The core has three main parts to it: functions, categories and subcategories. There are five high level functions: identify, protect, detect, respond and recover. The second part of the core are the categories, which are 23 different ones, split across five functions as illustrated in Figure [10] (NIST, 2020).

Figure 10

NIST framework core



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

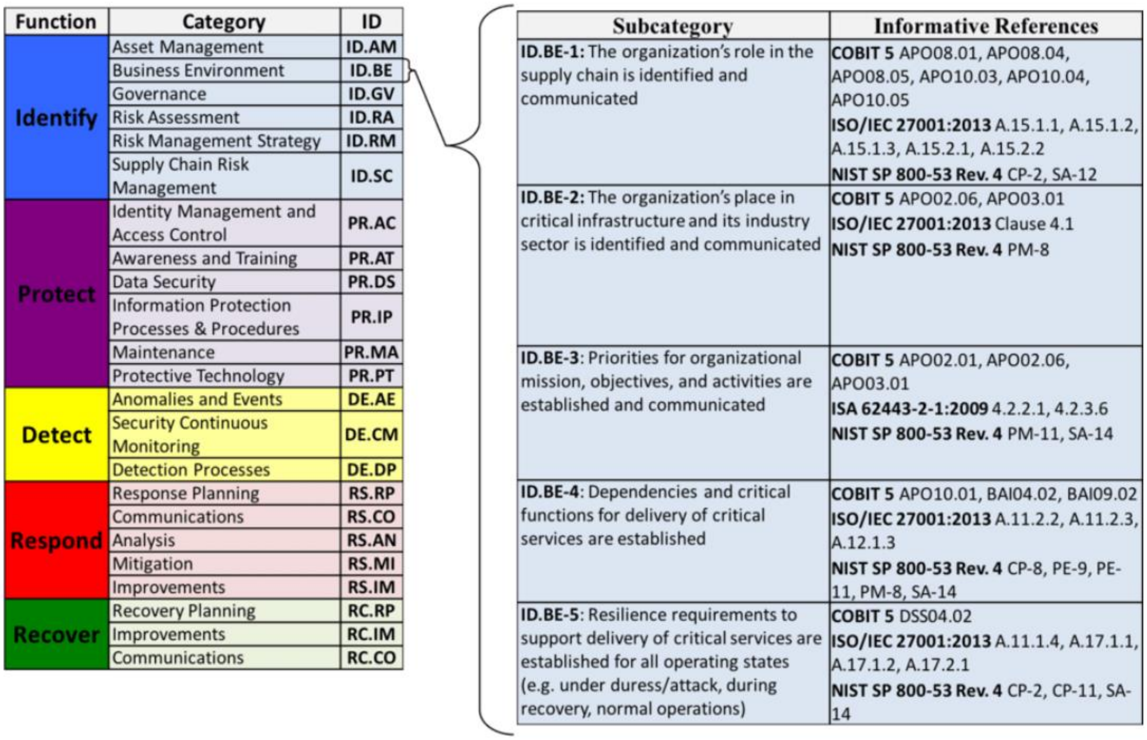
Copied from “An Introduction to the Components of the Framework” by NIST, 2020

The categories focus on topics such as cyber, physical and personnel, with emphasis on business outcomes. The category section was designed to cover cybersecurity as a whole, without being too complex or detailed.

The last part of the core is the subcategories, of which there are 108 different subcategories. These are outcome driven statements that provide considerations for creating or improving a cybersecurity program. Since the framework is outcome driven and not an official order on how the organization has to achieve these outcomes, it enables risk-based implementations that are customized needs of the organization.

Figure 11

NIST Core components with subcategories



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

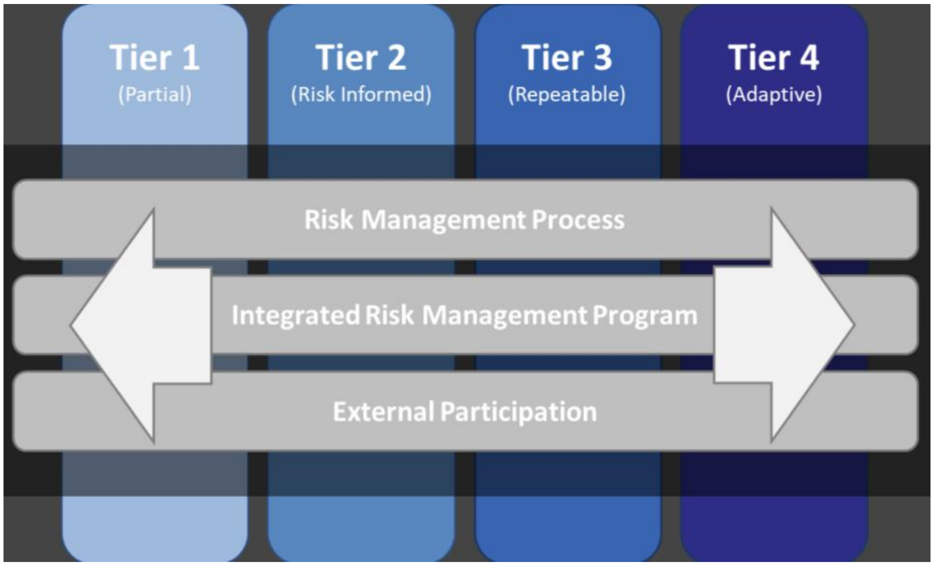
Copied from "An Introduction to the Components of the Framework" by NIST, 2020

The five subcategories in Figure [11] is an example of the outcome focus statements that are seen throughout the core. The informative references section support the core by providing a broad amount of references that are more technical than the framework itself. Organizations may choose if they wish to use these to achieve desired outcome in the subcategory (NIST, 2020).

3.3.2 Implementation tiers. The tiers section of the framework describes the degree to which an organization's cybersecurity risk management practices publicly displays the characteristics defined in the framework. There are four tiers, ranging from partial to adaptive, with an increasing degree of rigor. Organizations determine their desired tier, thus ensuring that the selected level meets organizational goals. Once the desired tier has been reached, it reduces cybersecurity risk to acceptable levels for the organization (NIST, 2020). The implementation tiers section feature can help with an organization's measure where it is currently positioned within the framework (Krumay et al., 2018, p. 226).

Figure 12

NIST implementation tiers

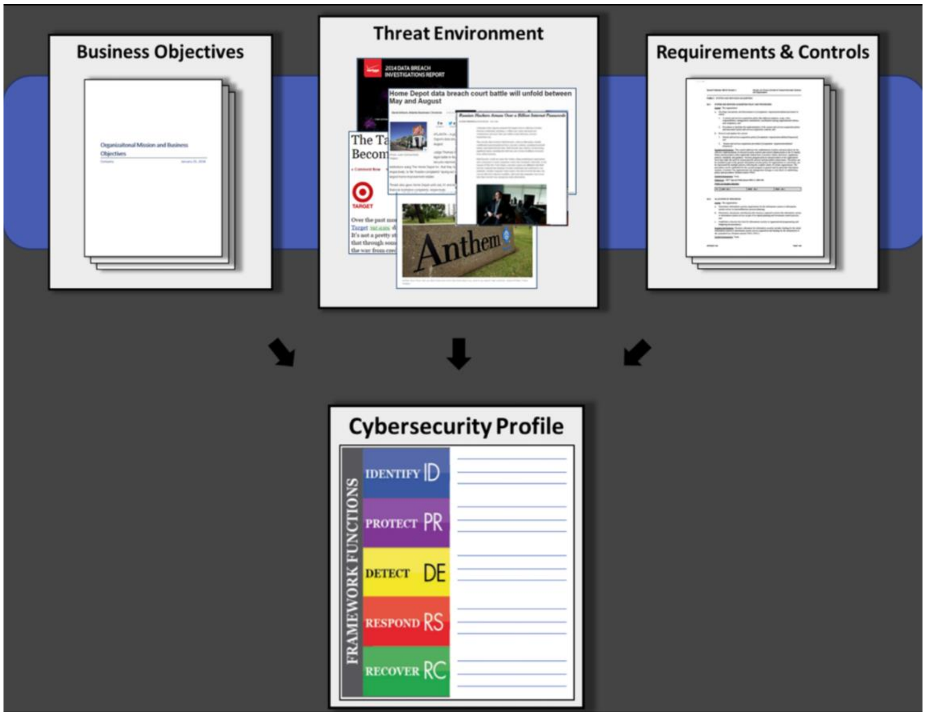


Copied from “An Introduction to the Components of the Framework” by NIST, 2020

3.3.3 Profiles. Profiles are an organization's unique collection of requirements, objectives, risk appetite and resources against the desired outcomes of its own core section of the framework. Profiles can be used to identify possibilities for improving their cybersecurity posture, by comparing a current profile with a target profile (NIST, 2020). The profile section represents the adjustments and priorities of activities and results for numerous industries and organizations according to their needs (Krumay et al., 2018, p. 226).

Figure 13

NIST profiles

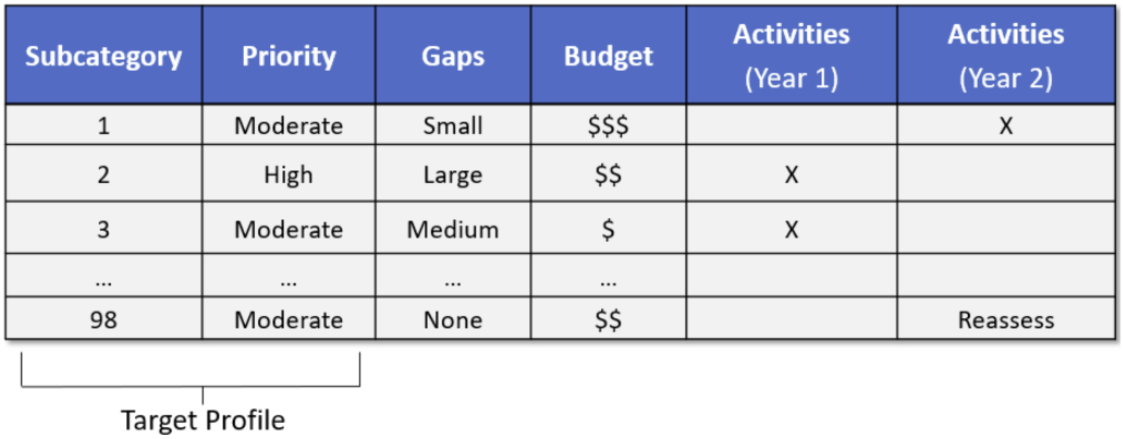


Copied from "An Introduction to the Components of the Framework" by NIST, 2020

The profiles are about optimizing the cybersecurity framework to best fit the organization. The framework itself is voluntary, which is why there is no correct way to handle profiles. One way to approach profiles is for companies to map out their cybersecurity requirements, mission objectives, operating methodologies and current practices to create a current state profile. The current state profile can be compared to the current operating state of the organization to gain a better understanding of any differences between the two.

Figure 14

NIST target profiles



Subcategory	Priority	Gaps	Budget	Activities (Year 1)	Activities (Year 2)
1	Moderate	Small	$$$		X
2	High	Large	$$	X	
3	Moderate	Medium	$	X	
...	...	...	...		
98	Moderate	None	$$		Reassess

Target Profile

Copied from "An Introduction to the Components of the Framework" by NIST, 2020

When these profiles are created, the gap analysis allows organizations to create a prioritized implementation plan. The priority, size of gap and estimated cost of the corrective actions helps organizations plan and budget for future cybersecurity improvement activities (NIST, 2020).

3.3.4 Advantages of NIST. According to NIST themselves, they have been observing how the community has been using the framework. They have reported that there have been common patterns along with the different communities. NIST reports that leadership has picked up the vocabulary of the framework, and can now communicate with proper terminology in conversations about cybersecurity risk. This is a major advantage as it lessens the distance to the people working directly with cybersecurity and the leadership. Another advantage according to NIST is that organizations have used the tiers to determine optimal levels of risk management. This ensures that the organizations are satisfied with their current risk management, and that everyone is in complete agreement about their cybersecurity. One major advantage NIST has is its voluntary and flexible nature. Cimpress-FAIR, who has had success with NIST, were happy with the way NIST measures risk, as they were allowed to take more risk when they accurately and consistently measure it (NIST, 2020).

3.3.5 NIST studies. In a study by Krumay, Bernoider and Walser (2018), the authors conducted a literature review consisting of 56 articles to evaluate cybersecurity management controls and critical infrastructures. The authors did this explicitly to find out if current reliance on established frameworks are sufficient. The cybersecurity framework in focus was NIST, where they aim to see how well the framework is covered by academic research, in order to pinpoint areas where additional research is needed (Krumay et al., 2018, p. 370). The authors say that critical infrastructures are the backbones of developed societies, and information systems have become vital for managing them. Given this situation, securing information systems directly influences the safety of critical infrastructures, which further emphasizes how important they are. According to the authors, the NIST cybersecurity framework is arguably one of the most important risk management frameworks in this regard. They did however find areas that needed more research, specifically in terms of metrics and controls. Additionally, they suggested a number of topics that seemed missing or underrepresented in the NIST cybersecurity framework (Krumay et al., 2018, p. 381).

Chapter 4 - Research approach

Research is an extensive process, and there is usually no clear path from A to B. However, with any type of process it is important to know how to proceed. A way to advance with a process is by choosing a methodology that is easy to follow (University of Southampton, n.d). There exist several different approaches to doing a literature review, the most common ones are narrative or traditional literature reviews, critically appraised topics, scoping reviews, systematic literature reviews and annotated bibliographies (Grant, M.J. and Booth, A., 2009). Grant and Booth attempt to clear up the terms review and literature to avoid confusion and incorrect use of both terms. Additionally, they review 14 different types of methodologies and list both advantages and disadvantages with each type. After understanding the different methodologies, we arrived at the systematic literature method. It is an approach that identifies, evaluates and chooses research to answer a clearly formulated question (Grant, M.J. and Booth, A., 2009).

In order to further strengthen the data gathered from the SLR, interviews were conducted with IT companies. By doing this, the thesis would not only present concurrent data, additionally it might present new points of view that have not yet been documented. There are several methods to conduct an interview; this paper uses a Semi Structured Interview (SSI). The style of an SSI is suitable for learning about the motivation behind people's choices and behavior, their attitudes and their beliefs. SSI is a technique to obtain valuable information that was not anticipated by the researchers (Raworth et al., 2019).

4.1 Research designs

For this study we chose to implement both exploratory research design and case study research design. Exploratory research design means to investigate a problem which is not clearly defined. It is created to get a better understanding of an existing problem, but will not provide conclusive results (Saunders, M., Lewis, P. & Thornhill, A., 2012). The idea behind exploratory research is to explore an area of which limited information is available. Data gathered in this type of research can be either quantitative or qualitative, with this study using interviews to collect qualitative data. The resulting data can be used as input for case studies that have the goal to present the findings in a categorized structure.

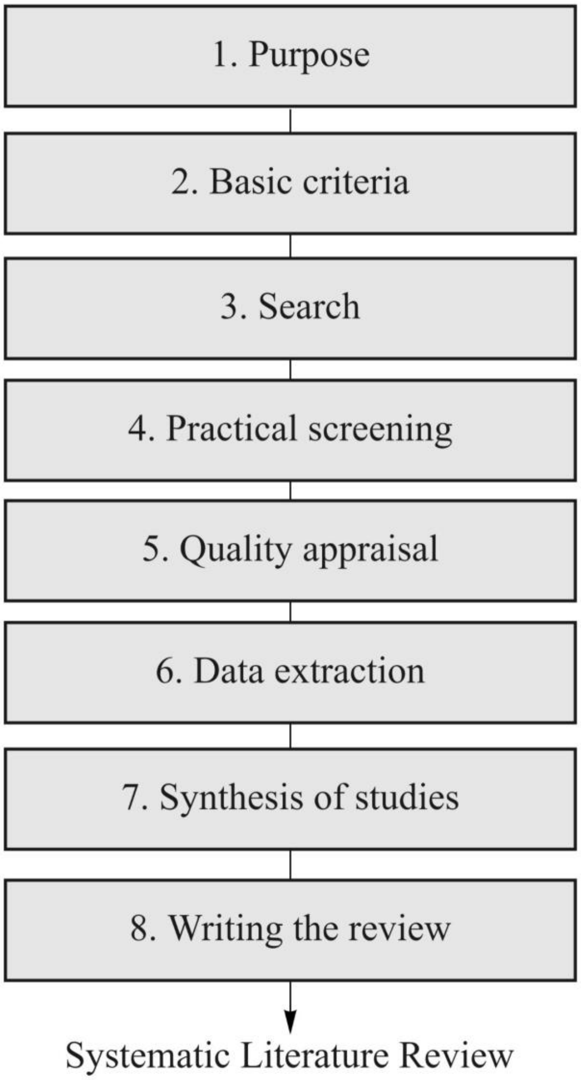
4.2 Systematic literature review methodology

An SLR starts with a clearly defined research question, which are questions that guide the thesis. The approach aims to discover all existing data on the subject in an unbiased, transparent and reproducible way. SLR creates research questions that are either broad or narrow in scope, then they identify and synthesize the studies that relate directly to the review in question (GET-IT Glossary, n.d.).

According to the article “Glossary for systematic reviews and meta-analyses", the SLR is a well planned and thoroughly executed literature review that analyzes findings from contemporary studies to answer the chosen research questions (Nagendrababu et al., 2020). SLRs are not perfect however, they have gotten critique for a number of things. This critique involves the requirement of a wide range of different databases, as well as peer-reviewed journals, which may be expensive for non-academic researchers (Mallett et al., 2012, p. 448).

Figure 15

Systematic Literature Review model



Created by E. Burkan & A. Tanase 2021

Figure [15] visually explains the different stages of the SLR, as well as the order in which it was executed and was inspired by a figure from a paper by Affia et al. (2019).

4.2.1 Purpose. A crucial part of any scientific paper is a literature review. This helps the author gain an understanding of any existing research and discussions that are relevant to the area of study (Western Sydney University Library, 2017, p. 1). For the purpose of this study, the literature review will help the researchers identify key aspects of cybersecurity analysis methods.

Not only is the purpose to identify key aspects, but also to evaluate and summarize the findings of all relevant individual studies (Gopalakrishnan, S. and P. Ganeshkumar, 2013). An SLR aims to identify and synthesize the most relevant scholarly research on the research topic. This allows for the unbiased gathering of scholarly evidence to support the claims presented.

4.2.2 Basic criteria. Due to the large volume of articles written on the topic of cybersecurity, it is not feasible to analyze each individual article. Therefore, we opted to formulate inclusion and exclusion criteria as recommended by Sage Publications (2020, p.51). This section will discuss the chosen criteria and explain the rationale behind them. The purpose of this chapter is to showcase which criteria are chosen for the literature review and why.

The chosen criteria are as follows:

- *No studies with a publication date before 2015*
- *Only articles and studies published in English*
- *At least a few citations, unless they are newly published.*
- *Research papers must contain one of the main topics.*
- *Both journal articles and conference papers are allowed*

The criterium of no studies published before 2015 was selected due to the aforementioned ever growing nature of the field of cybersecurity, we felt it was paramount to select only contemporary studies. Furthermore, the initial search results in the databases used for this review showed that the majority of articles were published in English. Thus, the choice was made to stick to English studies with the added benefit of reaching a wider audience. The criterium of articles requiring at least a few citations, unless recently published, in order to be considered eligible for inclusion was due to the increased chance of them being of sufficient quality. The main criteria was that the chosen articles would contain at least one of the main topics, and this is what the search phrases were based on.

4.2.3 Search. For this study we used the academic research databases Google Scholar, Microsoft Academic and Scopus. Determining the correct search terms posed a challenge due to the excessive number of articles available. When having a broad search it was noticeable that there were too many articles that were brought to light. This was problematic because it would require an unreasonable amount of time to thoroughly go through each one. Therefore, it was decided to use multiple keywords in the searches in order to narrow down the number of articles. Given that the topic of this thesis has multiple subthemes, several searches were required in order to cover them.

The finished searches in the different databases were relatively similar, however some small changes were done to get better results. Therefore, it was necessary to establish the keywords that had to be included in our search. The Google Scholar and Microsoft Academic search were exactly the same, whereas the searches on Scopus required alterations. Below is a table that shows the search queries used for the individual databases, together with the number of articles found.

Table 3

Search conducted on Google Scholar

Google Scholar SG = Search Google Scholar
SG1: "Cybersecurity analysis" Threat analysis Risk Analysis Penetration Testing Network and system monitoring Policies and security awareness - 60 articles
SG2: "Cybersecurity framework" OWASP ISO 27000 NIST - 67 articles

Table 4

Search conducted on Microsoft Academic

Microsoft Academic SM = Search Microsoft Academic
SM1: "Cybersecurity analysis" Threat analysis Risk Analysis Penetration Testing Network and system monitoring Policies and security awareness - 38 articles
SM2: "Cybersecurity framework" OWASP ISO 27000 NIST - 102 articles

Table 5

Search conducted on Scopus

Scopus SS = Search Scopus
SS1: Cybersecurity analysis framework economics - 19 articles
SS2: Cybersecurity analysis NIST - 42 articles
SS3: Cybersecurity analysis OWASP - 23 articles
SS4: Cybersecurity analysis ISO 27000 - 3 articles

We believe that by performing all of our research in this way, we were able to find relevant and up to date information surrounding our research topic. These searches provide the study with a good foundation and makes it relevant both today and hopefully in the future.

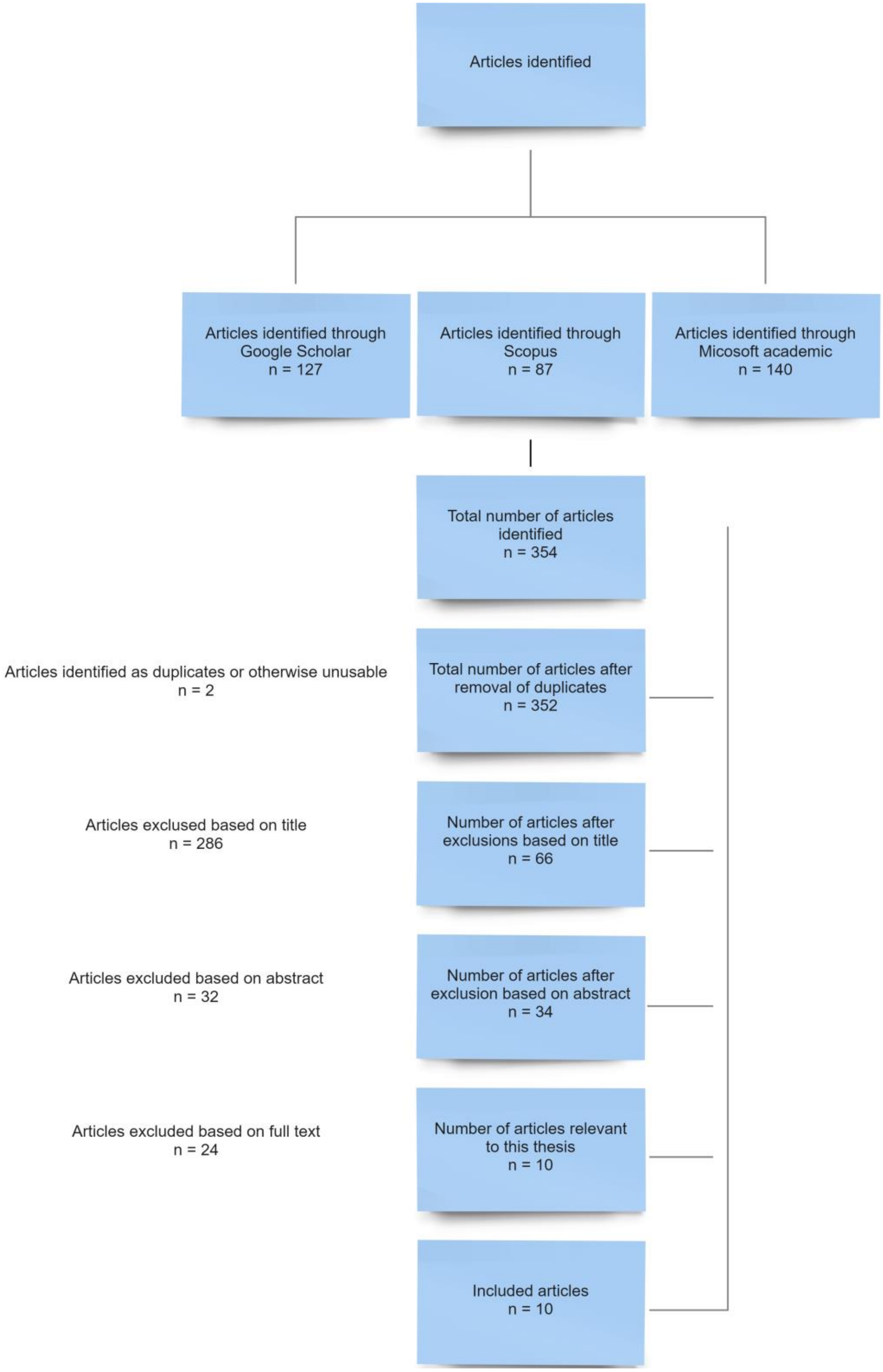
4.2.4 Practical screening. Conducting a practical screening for an SLR requires dedicated planning. Once the review is done, one is left with hundreds or even thousands of articles about the topic of interest. For this reason it is therefore impractical to read and analyze all of them in detail. The importance of the practical screening is that the reviewer must decide and explain on what criteria article judgement will be based (Okoli, & Smith, 2010, p. 21). The practical screening criteria applied in this study were as follows:

- *Remove articles that are duplicates*
- *Articles selected based on relevant title*
- *Articles selected based on relevant abstract*
- *Articles selected based on relevancy of content*

After conducting the search on all three databases, we were left with a total of 354 articles. The next step in the process was to look for duplicates, resulting in the removal of two articles. Next, inclusion was done based on title, leading to a total of 66 articles relevant to this study. The next step was to read through every single abstract to find the most relevant ones. When examining the abstracts, we were specifically looking for practical examples or a thorough explanation of the topics. Once that was completed, we were left with 34 articles. The last step was to read through all the remaining articles and only keep the most relevant. In the end we were left with a total of 10 articles, which we deemed the most suitable.

Figure 16

Systematic Literature Review process.


Articles identified
Articles identified through Google Scholar n = 127
Articles identified through Scopus n = 87
Articles identified through Micosoft academic n = 140
Total number of articles identified n = 354
Articles identified as duplicates or otherwise unusable n = 2
Total number of articles after removal of duplicates n = 352
Articles exclused based on title n = 286
Number of articles after exclusions based on title n = 66
Articles excluded based on abstract n = 32
Number of articles after exclusion based on abstract n = 34
Articles excluded based on full text n = 24
Number of articles relevant to this thesis n = 10
Included articles n = 10

Created by E. Burkan & A. Tanase 2021

4.2.5 Quality appraisal. Once the practical screening was finished and a set amount of articles were left, we determined the criteria for which of the remaining articles were worth keeping. The remaining articles need to be thoroughly examined, in order to assess their value and quality. In a way the quality appraisal is a second screening, which does not meet the standard of the reviewer. Not all the studies will be of equal quality, which is why it is vital to review and rate the studies according to the value they provide for the review (Okoli, C. & Schabram, K, 2010). Since the data collection has gotten narrower, it is important to be strict with the remaining articles. We did not feel the need to rate the remaining articles. After applying the inclusion and exclusion criteria, the remaining 10 articles were all considered to be an important addition for this study. Because of the amount of topics that this thesis covers we believe that it was necessary to include at least one article that provided a good theoretical basis for each topic.

4.2.6 Data extraction. After completing the quality appraisal of the chosen literature for this study. The next step in the process is data extraction. At this stage information and data is extracted from the selected literature sources and included in the study (Okoli, C. & Schabram, K, 2010).

The goal of the data extraction stage is to gather appropriate and relevant information to get accurate data for the thesis. The data extraction will be the foundation for the study, and the data extracted was mostly use cases of the different analyses and frameworks. Other general or generic information regarding the analyses and framework can be gathered from their respective websites such as OWASP, NIST or ISO. This further emphasizes the need for real life scenarios using these countermeasures, as the goal was to present the value of these countermeasures and compare them to each other.

4.2.7 Synthesis of studies. The synthesis of studies is the integration of existing knowledge on the subject at hand. Synthesis is important because it presents the articles in a polished way, which makes writing the literature an easier process than it would have been otherwise. Since studies can be either qualitative or quantitative there are different kinds of research synthesis to fit them both (Wyborn, et al., 2018). After gathering all the different studies the relevant data was extracted. The screening process left us with several articles with unique topics. The literature was grouped in their respective topic, if a study contained information about OWASP, the study would be written in the OWASP chapter. This ensured that the key concepts would be covered by information gathered from relevant and reliable sources.

4.2.8 Writing the review. The last step of conducting a literature review is actually writing the review itself. When writing the review, the authors need to carefully choose and present relevant and important facts and information from the chosen literature. The chosen literature needs to be supportive and to help back up the existing theory as well as contribute to further research (Okoli, C. & Schabram, K, 2010). The findings of the SLR are presented in chapter two of this thesis and will also be used in conjunction with the interview data.

4.3 Practical interview implications

In addition to planning and designing the study, it was also necessary to send in a NSD application. NSD is the Norwegian center for research data, which is responsible for managing all research projects and also offers an archive for research data. When in contact with NSD, they had to confirm and clarify certain elements in our thesis that were misleading. According to NSD's website, they give researchers advice on data handling, as well as wanting to improve the options for empirical research through a broad offer of data and support services. When NSD approves an application, researchers are legally allowed to store and document their data. Before data was stored or documented in the thesis, we made sure to get approval by NSD. To abide by these rules, this study has been approved by NSD with reference number 427166.

We did come across a few complications when contacting the companies for the interviews. Since we ask quite intrusive questions regarding their security, some or most companies were put off by the idea of an interview. Most of the companies we tried to interview had been through a strict security clearance and are not allowed to speak on the topic even though it would all be anonymous. This was completely understandable but made complications for the authors when seeking for respondents. We were however satisfied with the quality of the interviews that were conducted, nonetheless it would most likely be easier if the questions were not so intrusive from their perspective.

4.4 Case studies

Case study research methodology is a useful research method that can be used to explore a specific topic and present it from a holistic point of view. Case studies allow researchers to have an in-depth look at data found within a specific context. There are three different types of case studies: exploratory, descriptive and explanatory. The main differences between the different categories of case study is how the researchers present and explain the data gathered (Zainal, 2007).

For this thesis, it was appropriate to use exploratory case study, as exploratory case studies are meant to be used when researchers want to investigate a particular topic with little prior research. For the chosen topic, it was necessary to get more insight from the real world in addition to the literature collected. The exploratory case study was used to analyze each company interviewed, in order to get an understanding of how each company sees cybersecurity and to dive deeper into their understanding and experiences in this field. The case study attempts to explore the topic of cybersecurity analyses and the derived value of cybersecurity for IT companies (Gerring, 2004).

One of the advantages that a case study has is that they are designed to be done within the area of the topic of research (Yin, 1984). For instance, in this case, the objective was to see what value cybersecurity brings to IT companies. The best way to find out such information was to reach out to real IT companies and examine their experiences with cybersecurity. Another advantage of case studies is that they can be performed with a qualitative method, which was beneficial to this study due to the chosen approach of using interviews to gather data. Case studies also paint a larger picture by allowing researchers to explore real life phenomena, and to get a greater understanding for why things are the way they are (Zainal, 2007).

Having discussed the advantages of case studies, it is equally as important to also present the disadvantages. In a study by Yin (1984), it is mentioned that case studies are prone to be influenced by researchers, thus affecting the direction of the findings and conclusions of the study. In addition, Yin presents that case studies can sometimes be too long and difficult to conduct in a clear and structured manner (Yin, 1984). Another disadvantage of case studies is that they do not necessarily provide enough evidence in order for a scientific generalization to be created. This is due to not having a large enough number of subjects when conducting a case study (Zainal, 2007).

4.5 Interview methodology

For this specific study, we have concluded that a semi structured interview (SSI) would be best suited. The alternative would be either a structured interview or an unstructured interview. When conducting the interview, the goal was to have an open discussion and potentially learn things outside the scope of the questions, while simultaneously wanting a certain degree of structure. SSI is a mix of 'open and closed ended' questions, often followed up by how or why. Compared to a structured interview where one follows a structure, an SSI can dive into unforeseen issues or topics. They usually last one hour at most, this is to minimize fatigue for both the interviewer and the respondents (Adams, 2015, p.492-493). The interviews conducted for this study usually lasted between 30 to 50 minutes, which felt like a sufficient amount of time for both the interviewers and the people getting interviewed.

It is however important to note that an SSI has benefits and disadvantages. One of the major downsides when deciding to use an SSI is that they are extremely time consuming and intensive compared to other methods. This means that the interviewers need to come well prepared before the interview. Not only do they need to come well prepared, but they also need to follow the respondents' answers along with being flexible to keep the interview adaptable. SSI is perfect in certain scenarios, especially when the goal is to have open ended discussion.

Before conducting the interviews, the participants were notified that they would be recorded. Once the formalities were complete, the interview could properly start. As for the interview itself, the idea was that the interview would flow like a normal conversation and not have a rigid structure, which is why we believe the correct interview methodology was SSI. After the interviews were complete, an important step was to re-inform the interviewees about how their data would be anonymized. This agreement was part of the NSD application and details how the data gathered in the interviews is processed, as well as how it is presented in this thesis. The goal was to have little to no correlation between the data and their company, so that as little information as possible could be linked to the companies. This was not only important for the NSD application, but also to ensure the interviewees that the data could not be used against them in any way.

4.6 Selection of cases

We decided to start the process with what type of companies we wanted to target, which were IT companies. Since there are IT companies in all types of sizes that might influence the data gathered, it was important to map the companies based on different sizes. Ultimately there were three categories: small, medium and large. We based our categorization on the amount of current employees. In order to determine which companies were suitable and relevant to this study, Digin was used. Digin is one of Norway's largest Information and communications technology (ICT) clusters, with more than 90 companies. Looking through Digins' list, a list was created containing all relevant companies for this thesis mapped in by group size.

The next step was to create a draft of the contact email that would be sent to all the different companies. This email was important, as this would be the first point of contact with the companies. We reached out to several different IT companies, and a vast number of them expressed interest in the thesis topic, but due to security related reasons they could unfortunately not assist us with an interview. We were fortunate enough to get a hold of four different companies that shared some insights about their current security knowledge. These four companies were the building blocks of the case studies. These case studies are presented in table [6].

4.7 Interview questions

The interview questions were the basis for conducting our qualitative research. The questions would hopefully provide satisfactory and relevant information that can be used to answer the research questions. The questions were designed to follow a semi structured interview model and guide to a more open dialogue between the interviewer and interviewee. The questions had four different main topics concerning the company's overall security. For each of the main questions there were several sub-questions, to serve as backup in case the conversation did not flow naturally. The questions ranged from potential threats for their company to their current countermeasures and their general security culture. In between these questions, the participants were asked open ended questions regarding how satisfied they were with current security controls. Additionally, they were also asked to define the term “value” in cybersecurity in order to get a broader view of what this term means to IT companies in the context of cybersecurity. It turned out to be one of the more interesting questions, because the participants all had different definitions. The complete list of the interview questions can be found in Appendix [1].

Chapter 5 - Research profile

One of the criteria of this study for selecting informants was that the informants were representing an IT company. An assumption was made regarding the security of IT companies; Since they are an IT company they are most likely more aware of the cybersecurity aspect compared to non-IT companies who do not have technology as their core function, priority or focus. The chosen informants were all different IT companies of different sizes, therefore the research context is divided into the sizes: small, medium and large. The sizes of the companies are based on an estimated categorization on the amount of current employees. The data extracted from the companies has however been completely anonymized as agreed upon with NSD and the informants. All of the interviews were conducted through a video conference tool, as the current situation with COVID-19 made it inconvenient to conduct the interview physically. In compliance with the anonymizing of the companies, minimal information is provided in this section. The companies interviewed are real and the case study data was gathered through observation and interviews; but given pseudonyms. This chapter will introduce the parameters used in the case studies, as well as four IT companies of contrasting sizes who partook in the qualitative interviews.

5.1 Parameters used in case study

The most important parameter was that all of the companies were an IT company as emphasized earlier. Another parameter was the size of the companies, which ranged from small to large. The idea was to discern whether the size of the company mattered in regard to their security and security culture. The reason it is beneficial to delegate the companies into different categories is because it might make it easier to map dissimilarities between them. When sorting the companies into the different categories it was difficult to exactly know how many employees they had, which is why the numbers are an estimate. The small size category had somewhere between 0-20 employees, the medium had 20-250 employees and the large category had 250 or more employees. The small size category can represent newly founded companies or companies that want to stay small. Medium size category represents known companies that may be family owned, but they might also be complex entities. The large category represents well known companies which are usually complex, often having connections to other companies and acting as a link. Another parameter worth mentioning was the company's location. There were no requirements as to where companies were located, but could provide useful information to see similarities or contrasts depending on their location.

5.2 Description of case studies

Table 6

Summary of case study

Companies	**Field**	**Size**	**Location**
DevelopedIT	IT, web development, transportation	Small, three employees and consultants	Norway
RegionalTech	Municipality and county IT services	Medium, 50 to 200 employees	Norway
ScandIT	IT, business consulting	Large, more than 500 employees	Scandinavia
FinanceIT	Financial	Large, more than 7000 employees	Norway

5.2.1 DevelopedIT. The first company that was interviewed was a small IT company that was newly founded and is classified as small. At the time of the interview they had three full time employees and some consultants that helped in case extra assistance was required during a frantic time. Two of their full time employees are located in Norway, while the other employee resides in another country. Originally they started their company to develop websites, but quickly offered a larger variety of services. DevelopedIT works with transportation and developed an application to manage transportation data. They maintain and manage large amounts of data of their customers, which is why it was both interesting and important to see how they handle their cybersecurity. DevelopedIT mainly operates in Norway, although they are open to do work assigned to them outside of Norway as well.

5.2.2 RegionalTech. RegionalTech is a medium size company with somewhere between 50 to 200 employees, and operates in the public sector. They are responsible for the operation of all ICT services in both municipalities and counties and offer services to their customers and owners. RegionalTech offers work in customer support, operations, network, project management, etc. They manage over 40 000 customers within Norway, which made them an ideal candidate for this study. One of their core values in the company is to be trustworthy, while striving to be as professional and to openly communicate to their stakeholders. As of today they have a responsibility over all population data, in their designated communes. RegionalTech owns a plethora of other companies who all operate in Norway.

5.2.3 ScandIT. ScandIT is a company that is classified as large, with more than 500 employees, and has operated for a long time. ScandIT owns numerous other companies which offer other services unique to ScandIT. They focus on new technology to create a sustainable future, because of this they hire several student graduates to stay on top of the current technology trends. They handle a great deal of different types of data which made them an excellent choice for this thesis. ScandIT operates around Scandinavia where they work in the financial, insurance, health and energy sectors to name a few.

5.2.4 FinanceIT. FinanceIT is another company categorized as large with more than 7000 employees within the financial sector and operates in Norway. Although FinanceIT is not directly an IT company, they have their own IT department and are committed to upkeep internal security. FinanceIT undoubtedly handles important information concerning the Norwegian population, which is why it is an area of concern. They have several divisions in the company that cover unique subjects in specific areas as well as nationwide. The division that was interviewed for this thesis was the IT department, which is apparent in all the other areas of the company. FinanceIT wants the IT division to function and support their vision both short and long term.

Chapter 6 - Findings

This chapter presents the findings of this thesis. The findings are based on the data gathered through conducting and transcribing the interviews as well as the SLR. There were six respondents from a total of four different IT companies, ranging from small to large, that participated in the interviews. The goal of the interviews was to ask IT companies about their current cybersecurity situation, so that it was possible to get a holistic perspective about how companies manage their cybersecurity. The main findings have been summarized in Table [7], with accompanying in-detail descriptions that help the reader understand the context of the results. The findings will be compared and analyzed to see if there are any relationships or differences between the companies. Furthermore, the chapter also dives deep into each of the interviews and attempts to connect to the research questions.

Table [7] introduces four unique companies and their size, with five different topics. These headings are meant to summarize how the different IT companies see the current cybersecurity landscape, and how they manage their cybersecurity needs. As mentioned in the introduction, value is a broad term, and we asked the companies how they define value in connection to cybersecurity, which is presented at the end of the table. Below the table there will be a more in-depth description of all the headings and more data dissected from the interviews, such as the company's thoughts and habits surrounding cybersecurity.

Table 7

Summary of qualitative interviews

Company	**Size**	**Possible threats**	**Security countermeasures**	**Data assets**	**Security frameworks**	**Company's definition of value in cybersecurity**
DevelopedIT	Small	DDOS, lack of availability, human error	Built in security tools, outsourcing security	Positioning information PII	None	Unspecified
ScandIT	Medium	Human errors, different security cultures	SOC, XDR, inhouse security	B2B data, PII	NIST, ISO 31000	Strategic, financial and organizational objectives. Understanding value in terms of opportunity
FinanceIT	Large	Foreign states, economical criminality (e.g., ransomware)	SOC, SIEM, SOAR, EDR, hybrid security	PII	NIST, NSM	Value of cybersecurity is the result of the investments required to keep information secure
RegionalTech	Large	Social engineering, malware, ransomware	Awareness raising, outsourced SOC and security measures	PII	ISO 27001, NSM & SANS Critical Security Controls	The value is to protect information and services that are valuable to the company and other actors related to them

6.1 Possible threats

One of the areas that the interviews focused on was finding out if the companies had any knowledge of possible threats. Threats can be anything from exploiting human error, to attacks from foreign states, and more.

DevelopedIT specified that they felt most threatened from attacks that may harm the availability of their product and system. They mentioned that such attacks could come from potential competitors. Another possible threat that was mentioned was human error. DevelopedIT said that since they are a small company with few employees, they do not worry so much about this. But if they grow, this could definitely pose a larger threat.

ScandIT mentioned that they see human understanding and capacity as their biggest security threat. Since they are a large company, they mentioned that they focused on creating a good security culture to combat any threats and risks related to the human attack surface. ScandIT also mentioned the importance of not blindly trusting suppliers of software, and always checking the security of software patches before implementing them.

FinanceIT's potential threats differ from the other respondents, and were based on their size and field. FinanceIT mentioned that for their company, foreign countries and financial crime are the biggest threats. They are also aware that threat actors might not necessarily want to attack, but are looking at ways to infiltrate FinanceIT's systems and possibly prepare for an attack in the future.

RegionalTech mentioned that they sometimes are targeted by DDOS, malware and ransomware attacks, but see the human factor in the organization as the biggest threat. RegionalTech further emphasizes that no matter how secure your system is, from a technical point of view, it will not help in case of human errors and exploits. If an organization has a good security culture and the employees have good security awareness, an attack may be prevented from even happening in the first place.

6.2 Security countermeasures

When talking about security threats, it seems only natural to also look at what security countermeasures the different respondents utilize. This is in order to find out which countermeasures real companies use, and why they have chosen those specific ones. Security countermeasures are very important when combating the ever growing security threats that face an organization. It is therefore crucial that when choosing which security measures to implement, thorough research and analysis is done in order to make sure that the chosen measures help mitigate the preexisting risks without bringing any new ones. Standards such as ISO, NIST and OWASP can help the company categorize their existing threats and find out which areas need improved security. From what we were able to find, the standards however do not say anything about the importance of testing new countermeasures when implementing them in an existing IT system. This topic was touched upon by most of our informants, as they felt it is important for them to test new security countermeasures and new services when adding them to their IT system.

DevelopedIT mentioned that until now they mainly outsource their cybersecurity. Their CTO mentioned that he does not feel comfortable enough to take full responsibility for the security and would rather outsource security to a service provider they can trust. Instead of doing a poor job themselves, they can just let the service providers deal with the security issues. They specified however that in case they will grow in size, they will eventually require personnel that focus on security.

ScandIT talked about how they use segmentation between the client data and internal operation data, as well as segmentation between automated processes and human interaction with the system. The interviewee said, “do not mix your network operation center and security operation center”, which puts further emphasis on their segmentation. They use this in order to minimize vulnerabilities and risks across their system. In addition to segmentation, ScandIT also has a security operation center (SOC) that helps them monitor their system against cyber attacks.

FinanceIT has more advanced security countermeasures. They utilize Splunk which is connected to a security orchestration, automation and response (SOAR) service to automate the handling of cybersecurity incidents. FinanceIT also utilizes a SOC that helps them achieve 24/7 protection against cyber attacks. In addition to the countermeasures already mentioned, FinanceIT also uses endpoint detection and response (EDR) software on the individual computers and servers of the company. The EDR software is connected to Splunk so that any malicious activity is logged and monitored.

As some of the other companies in this study, RegionalTech also outsources a SOC service that helps them be protected 24/7. They mentioned that they are preoccupied with having full end-to-end security. RegionalTech did not divulge what specific software or technologies they use.

6.3 Data assets

Data assets are the type of data the different companies strive to protect, the common data assets for all the companies were personal identifiable information (PII), along with a few more. Data assets are important as they say what kind of data the companies are responsible for if a data breach would happen.

DevelopedIT has access to data sets that includes information such as locations, driving history, braking distance, etc. This information is related to heavy vehicles such as trucks, trailers and excavators in Norway. Not only do they have information on the trucks, they also have information about all of the drivers.

ScandIT mentioned that they only have business to business data and PII. ScandIT said that there are no laws that inform how one should treat data related to customers aside from the privacy act. They said that they follow GDPR regulations.

FinanceIT said that they have all sorts of data that is in the population register, which is mostly what they are focused on protecting. They have logging and monitoring systems to see and record who takes a look into this type of confidential data.

RegionalTech did not specify what kind of data or data type they manage, however we learned that they supervise large amounts of PII. This is due to the nature of their business requiring them to collect and store different sensitive information of their customers.

6.4 Security frameworks

One of the core elements of this study is to scrutinize the typical cybersecurity frameworks adopted and applied actively in each company interviewed. Are there any relations between the size of the companies and their tendencies to adopt particular cybersecurity frameworks? The interview results indicate that most of the companies used NIST or “NSM’s grunnprinsipper” which are a set of Norwegian guidelines and principles to protect ICT security.

DevelopedIT did not have a specific framework they followed, however they believed they practiced safe coding and kept their software and packages up to date.

ScandIT were previously focused on the ISO 27000-series framework but are now generalized based on NIST. They prefer NIST over other security frameworks because it is so scalable. ScandIT also implemented ISO 31000 which is a framework for all risk work and risk management tools, over spreadsheets.

FinanceIT also utilizes the NIST security framework, along with “NSM’s grunnprinsipper”. Their opinion on the matter was that it is best to follow a Norwegian security framework, as they are made to cover the needs of Norwegian companies that operate within the Norwegian rules and regulations.

RegionalTech operates with: ISO 27001, “NSM’s grunnprinsipper” and SysAdmin, Audit, Network and Security (SANS), according to them those are the standards that are the best practice which most other companies use to compare their security expertise. RegionalTech mentions that both ISO 27001 and NSMs mapping tables are easy to work with. They appreciate how easy it makes it for them to know where they stand in terms of security and what they need to do to improve their security through the implementation of the standard. They believe that NSM does a good job to Norwegianize security terminology, which makes it more appropriate and understandable for Norwegian companies.

6.5 Definition of value in cybersecurity

At the end of the interviews a question about what the companies define as value in relation to cybersecurity arose. The idea behind this particular question was to gain insight into what the different companies deem as valuable related to cybersecurity.

DevelopedIT did not have an answer to this, because they were recently established and did not yet put any thought into it. ScandIT had a lot to say about this topic and compared to DevelopedIT had put plenty of thought into this beforehand. ScandIT split the answer in three parts: strategic, financial and organizational objectives. ScandIT said that these can be fulfilled through three risk aspects, which were: business risks, legal and compliance risks and loss of trust. Additionally, ScandIT said that it is important to understand value in terms of opportunity.

FinanceIT defined cybersecurity value as the total gathered value of the data that an organization deems important. An example of why it would be important is that some data is so valuable that it cannot be lost or that it is to be kept secret and away from the public. FinanceIT finished off by saying that the value of cybersecurity is the result after an investment, along with the reasons as to why you have invested to keep data and information secure.

RegionalTech defined value as “why would we want this specific countermeasure?”. It is to protect information and service that may have a value in the company and its stakeholders. They also did a value evaluation to find out in which order they prioritize services and systems and use that data to implement security measures. RegionalTech concluded that the information is worth just as much as gold, and it is important to protect the most valuable data.

6.6 The respondents thoughts and habits regarding cybersecurity

We asked DevelopedIT what they thought would be the benefits of doing an analysis for them. They were open to discussing this with us, and said “A security analysis would be most beneficial by helping us find new potential vulnerabilities and categorize them”. Although, given the size of their company they stated that such an analysis would not be of great value at this point in time. They believe that some security mistakes originate from the human aspect of the company, which is why they would like to implement policies if they had more employees.

ScandIT uses a qualitative risk model which is all about counting until you have a risk value. It is not about if you have a long password or not, it is more about if you have 2-factor authentication or if you have the proper security culture in place. They also have a security slogan that is “prevent, protect and try”. ScandIT said that “You can't operate through reactive work, you need to do proactive security work.”

FinanceIT stresses the importance of 24/7 surveillance as threat actors do not go when normal people do, because they might not have the same responsibilities. They use risk and vulnerability analysis multiple times a year, where some of the things they look at are threats both inside and outside of the company. When they create a new service, an analysis is done preemptively to look for any flaws in the service.

Performing a cybersecurity analysis can benefit a company when choosing what new software and services they want to use. After such an analysis is done, they have the possibility to have an overview of potential vulnerabilities, or areas where they need to improve. This is what motivates RegionalTech to run analyses and to test their systems regularly. It is the results of these analyses that are the foundation of any decision making inside the company.

Chapter 7 - Discussion

This chapter is meant to review the results of the interviews presented in chapter five and compare them to the literature used in chapter two. It is important that these findings are discussed and analyzed in order to help answer the thesis's research questions and; "*How does an IT company perceive the value of cybersecurity frameworks?",* "*What are the challenges of conducting a cybersecurity analysis?"* and *"How can performing a cybersecurity analysis benefit an IT company?*". Additionally, help raise awareness of IT companies on which frameworks and cybersecurity analyses are suitable to improve the company's security.

The chapter is split up into three segments, where the first segment will present a more detailed explanation of the term value in a cybersecurity context and compare our definition to the definition of the respondents. This first segment also discusses how any complications regarding the use of cybersecurity analyses and frameworks can affect the value derived from the use of such analyses and frameworks. The second segment of this chapter discusses the limitations related to the thesis as a whole. Lastly, the final segment presents this thesis's goal to contribute to the already existing research on the cybersecurity subject, more specifically cybersecurity analyses and frameworks.

7.1 Value of cybersecurity analyses and frameworks

The value aspect in regards to cybersecurity analyses and frameworks almost always addresses economical value in some way. When conducting the literature review we did not specifically look for literature that only concerned the economical aspect, but also other aspects of value.

Through this thesis we contribute to the subject on how valuable cybersecurity analyses and frameworks really are. Furthermore, we recognized that there were more areas to look at than just economical aspects. An example of those aspects would be the potential to say you are ISO-27001 compliant. This may be of value for some companies, as ISO is a respected and well known framework. These aspects are important to recognize when deciding what kind of value each of the chosen frameworks and analyses provide.

7.1.1 Threat analysis. McCabe (2007) lists a number of assets that could be vulnerabilities, as well as threats to those assets. The value a threat analysis can provide is the knowledge of identifying which assets may be vulnerable and what types of threats may pose danger to those assets. If one were to analyze this more in-depth, there would be multiple types of value a threat analysis contributes to. The main value a threat analysis brings is the economic advantage, since the cost of implementing a threat analysis might be cheaper than the anticipated cost of failure. If a company does not conduct a threat analysis, they could receive repercussions for it. An example of the repercussions could be loss of trust in the company name.

RegionalTech and FinanceIT both use threat analysis to achieve a clearer overview of their threat image, which offers the companies the possibility to invest in the appropriate areas. Both companies mention that a threat analysis is not enough to uncover all vulnerabilities and risks, but it is a great starting point for companies that wish to achieve a better level of security.

7.1.2 Risk analysis. Risk analysis is somewhat of a continuation of threat analysis. Instead of evaluating what vulnerabilities might be exploited, the risk analysis attempts to recognize the probability of a vulnerability being exploited. This is important to take into consideration if a company wants to conduct a risk analysis, as the analysis might bring zero value unless the vulnerabilities are already mapped out. Risk analysis is a complicated process where prior knowledge is necessary. It is also required to have both knowledge and practical experience in the field where the analysis is conducted (Czechowski, 2016, p. 24-25). If the required information is available, the risk analysis will be beneficial to companies so that they know where to focus their attention. Specifically the type of value it can bring is mainly economical, as it can aid with preventing big risks from developing. Additionally, risk analysis can provide value since companies might manage data which is not economically dangerous to lose. However, it can harm the company in other ways, such as their reputation.

RegionalTech was very talkative about this process, and said that they use risk and gap analyses when wanting to implement new tools and software into their system. They feel like these analyses give them a good overview over the areas where they need to improve security. DevelopedIT also had a similar approach, although on a smaller scale given the size of the company. The respondents said they find that the value of risk analysis comes from the information about how malicious a threat can be.

7.1.3 Penetration testing. Penetration testing is not directly an analysis, however it was easier to group it in the analysis section as it also includes a type of analysis in the aftermath. The idea behind a penetration test is to look for potential vulnerabilities in system configurations, hardware or software to name a few (Bacudio et al., 2011, p. 19). Penetration testing will be valuable for companies looking to find actual security flaws in their system, and get advice on how to fix these flaws. It might be more expensive and more time consuming than other types of analyses, however the accuracy of finding the real vulnerabilities are valuable. Conducting a penetration test for a company makes them the center of attention, and may find flaws specific to that company. Compared to other, more generic, solutions which may not cater to them. The value of penetration testing lies in several areas, however the one that we want to highlight is that companies have the option to test their system as if it were a real cyber attack. This might result in economic value, since the company gets to prepare or solve any undiscovered underlying issues.

RegionalTech was the only company from the interview that actively used penetration testing as a method for improving their security. They mentioned that they have a contract with a third-party supplier for penetration testing to regularly perform tests on RegionalTech’s systems. Upon completed penetration tests, RegionalTech gets delivered a complete report over the vulnerabilities and security flaws that the third-party supplier has managed to find. RegionalTech specified that they find great value from third party penetration testing in particular. They meant that this is valuable because it tests their systems against real life scenarios, which helps them further improve their security.

7.1.4 Network and system monitoring. Network and system monitoring is about monitoring different parts of a company. Through this process it is possible to detect unnoticed software vulnerabilities, errors and other security related issues (Lv et al., 2018, p. 27). All of the companies interviewed, except for DevelopedIT, use network monitoring through well known applications such as SOAR and SIEM applications. The value monitoring can provide is beneficial, especially when companies want to learn from past mistakes or look up potential vulnerabilities in the current system. Inspecting logs through applications such as Splunk gives the possibility to execute post error investigations. It provides an opportunity to determine the cause of a certain error or cybersecurity breach. This could grant economic benefits by ensuring that the problem will not happen again. Additionally, it can help notice current complications faster compared to no monitoring of the organization's network or system.

7.1.5 Policies and security awareness. Policies and security awareness controls serve as rules or guidelines that employees of a business must follow while working within the company. Being aware of security is essential for companies, so that the employees might think critically about how to approach certain scenarios. Wigmore and Ivy (2017) discuss why organizations should be aware of the human attack surface To emphasize on this, ScandIt mentioned in their interview that the importance of human capacity and understanding must not be taken lightly. In order to prevent cyber attacks from happening it is important to provide training for the employees to help them achieve a desired level of security awareness. Furthermore, the paper by Höne and Eloff (2002) also discusses how one should create good information security policies that help raise the security awareness within the employees of a company. Höne and Eloff mention that the policies should be created in accordance with the security standards like NIST and ISO 27000, that have been central throughout this thesis.

In addition to policies, Grassegger & Nedbal (2021) present the importance of a holistically secure IT system. One important way through which companies can potentially achieve holistic security is creating a strong security culture. Most importantly it was interesting to see that the companies we interviewed also shared the same ideas surrounding the value which a holistic view on cybersecurity can bring to an organization. Especially the versatility of security culture and security awareness that can be achieved through fewer monetary investments, than for example a risk analysis or penetration test.

The value of security policies, awareness and culture helps lessen the risks related to the human attack surface (Wigmore, Ivy, 2017). One specific value of security policies is that they can potentially be a free security measure to implement for a company. Although it is still important to consider that the vulnerability will always be there regardless of the policies. Established security culture promotes good security without necessarily requiring continuous monetary investments which is where the value mainly lies.

7.1.6 OWASP. OWASP created a list that contains 10 common flaws and security risks that web applications may be vulnerable to. They provide guidelines to avoid these flaws, meant to be followed through a development cycle to avoid the Top 10 list (Arya Wiradarma & Arya Sasmita, 2019). The community surrounding OWASP is continuously growing and especially interested in cybersecurity. Compared to every analysis or framework in this thesis, OWASP is the only tool that is open source and ready out of the box for everyone to use. This makes it highly valuable for almost all companies, but especially the ones with less economic capabilities. What adds to the value is that OWASP continuously updates their Top 10 list, so that the companies who use the framework do not follow outdated guidelines. OWASP ought to be combined with other types of analyses, such as a risk analysis to be even more useful. Unfortunately, OWASP as a subject was not a focus during the interviews, due to the fact that none of the respondents actively used this framework.

7.1.8 ISO 27000/27001. The global recognition most ISO standards have are valuable for any type of company. The last publication of ISO 27001 was in 2013, and is familiar around the globe. The goal of the standard is to provide guidance for companies, so that they have a better basis for choosing their cybersecurity solutions (Renvall, 2018, p. 38). A valuable trait the ISO 27001 standard has is that it can be flexible especially towards small or medium sized companies, without incurring significant financial expenses. It might not be too challenging for companies to become ISO 27001 compliant, as the users do not need to be compliant with all of the controls, but only the ones they themselves choose (Renvall, 2018, p. 47). When a company can call themselves ISO 27001 compliant it provides value as they will seem more trustworthy compared to those who are not compliant. ScandIT mentioned that they previously were focused on utilizing ISO 27001, but recently shifted their focus on the NIST framework.

7.1.9 NIST. The NIST framework strives to help organizations manage and reduce risks through a flexible and complex system. NIST themselves report that the management team gains knowledge about cybersecurity vocabulary, which is valuable especially for larger companies. The CISO of ScandIT said that he had previously seen the effectiveness of NIST in another company which was one of main reasons why the change was endorsed. Furthermore he emphasized the value of scalability and flexibility derived from the NIST framework. They recommended it to any company regardless of their size. A small or large organization independent of their cybersecurity budget, can find an approach that fits them specifically. Just like ISO, being NIST compliant provides value. Particularly because being NIST compliant is meaningful, as it is a well known framework especially in the cybersecurity environment. Another valuable selling point of being NIST compliant is that it will help ensure that an organization's infrastructure is secure. During the interview with FinanceIT they revealed that they use NIST along with "NSMs grunnprinsipper". They feel that the combination of these frameworks gives Norwegian companies that operate within Norwegian law a better foundation for security.

Table 8

Summary of value of analyses and frameworks

Threat analysis	Economical value, overview of threat image & knowledge of vulnerable assets
Risk analysis	Economical value & information regarding malicious threats
Penetration testing	Economical value & simulate a real cyber attack
Network and system monitoring	Economical value, learn from past mistakes & monitor real-time issues
Policies and security awareness	Economical value, avoid human error, potentially free & adequate security culture
OWASP	Free resource, large community & continuously updated
ISO	Can help improve security, easy to follow, flexible framework & recognized globally
NIST	Can help secure an organization's infrastructure, flexible & recognized globally

7.2 Challenges for applying cybersecurity analyses and frameworks.

Given that one of our research questions was to study the challenges of conducting security analysis, it was not straightforward to take generalization from the informants. It was clear however that there are different attitudes and perceptions on how to implement cybersecurity countermeasures. These attitudes and perceptions may be influenced by the nature of their data assets (confidential, sensitive, PII), size of the companies, complexity of IT infrastructure, etc.

An important factor to take into consideration is the size of the company, which can make the difficulties vary. While a small company might not have enough resources to tackle the security issues, a larger company may have a very complex system that they wish to protect, thus requiring a greater number of resources. When this topic was discussed with our respondents, the idea was to figure out how they defined resources. All companies responded approximately the same when they defined resources: they implied time and money. RegionalTech elaborated that the size of the company is instrumental when uncovering how much a company should invest in internal cybersecurity measures. Quoted from RegionalTech, “There is no point in just doing it sloppy. You either do it properly yourself or outsource the task to someone that can deliver a higher quality service”. RegionalTech mentioned that since the threats are constantly evolving, it can be difficult for small size companies to keep up with the new technologies and the threats and vulnerabilities associated with them. As mentioned previously, DevelopedIT is a small size company and share a similar opinion to RegionalTech. Mostly because they do not feel comfortable enough with handling security in-house. Instead of doing a poor job themselves, they chose to outsource their security.

For larger companies such as ScandIT and FinanceIT, the complications do not necessarily fully originate from the limited sources of money and time. But rather the complexity of the preexisting IT system that may cause difficulties. ScandIT mentioned during their interview that it is important for a company to always maintain a holistic view of their organization. This is to know which potential threats and risks they are vulnerable to. They compared an organization's security countermeasures with the Norwegian army, and explained that it is important to know where the threats may potentially come from and design and implement security countermeasures in conjunction with that. ScandIT also gave an example of how one should look at investing in countermeasures. They said, “If someone works in a kiosk, they probably do not need a SOC to deal with their security threats. Compared to a larger company such as Hydro or the Norwegian Oil Fund”.

7.3 Limitations

Identical to almost every study there are important limitations to discuss. This study has a few important limitations that future research is encouraged to solve or improve. The most obvious limitation is the amount of analyses and frameworks included in the thesis. There are several analyses and frameworks available that are not included in the study mostly due to the time limitations. The goal for this thesis was to serve as a guide on cybersecurity analyses and frameworks for IT companies, but given the time available it was unfortunately not possible. Something to note regarding the interviewees, was that they mostly consisted of the company’s security management, therefore it is important to consider that they do not necessarily represent the security beliefs of the whole company.

Another known limitation with the study was the quantity of interviews conducted, mostly because of two causes. Firstly, it was challenging to get the companies to talk about security related subjects as it is a sensitive topic. We were rejected on multiple occasions because of the nature of our thesis and questions, even though we signed a non disclosure agreement beforehand and anonymized everything. Despite the aforementioned limitation being restraining, if there were more time we would eventually get more companies to interview, which was the second cause of the limitation. With the amount of interviews available it was difficult to draw conclusions. Along with the difficulties regarding the conclusions, it was also challenging to give recommendations to IT companies, the challenge arose primarily from the lack of data available. Regardless of the challenge, some recommendations were given as part of the conclusion.

The last limitation identified was that the questions during the interviews should have been more related to the theoretical background of this thesis. The questions asked during the interview were more generic and gave a broader view, but could have provided more data related to specific information regarding chosen analyses and frameworks of the companies.

In hindsight, if we were to rewrite the thesis many of the same limitations would have arisen. It is important to be aware of limitations, as it might provide an opportunity for further research to be improved (Price & Murnan, 2004, p. 66-67).

7.4 Suggestions for further research

If other authors were to continue research on a similar topic, we recommend to use analyses and frameworks not included in this thesis to hopefully reach an even bigger audience. If future researchers wish to continue on this thesis's original idea with creating a guide, the new findings need to be more organized and a road map would have to be created. The road map should include all established analyses and frameworks, in addition an idea would be to have a start and end point to the guide.

Another suggestion would be that future researchers gather more data from the interviews. The reason for this is to potentially provide enough data, to such an extent that it is possible to give more recommendations related to additional analyses and frameworks for IT companies.

The last but maybe the most important suggestion would be to recreate the interview questions, so that the questions focus further on the analyses and frameworks chosen in that particular research.

7.5 Suggestions for practice

It is difficult to recommend security solutions for companies that are well established. Nonetheless, free tools similar to OWASP are always worth taking a look at, especially when they publish a new top 10 list. We recommend every company to know their threat image and where their risks lie through tools for risk and threat analysis. The large companies, ReginalTech and FinanceIT, both follow "NSMs grunnprinsipper". We would recommend other companies follow their countries security guidelines similar to what the larger companies interviewed in this thesis did. We see value in flexible frameworks like ISO and NIST, as they can be adopted by companies of all sizes. Through policies and security awareness companies might avoid simple human errors, and can be economically advantageous in comparison to other frameworks or analyses. In addition, they can promote a good security culture within the company. RegionalTech finds great value in penetration testing, because they can test their system against real life scenarios, further developing their security. A recommendation from us is that more companies should look into penetration testing of their systems. This could prepare companies, so that they are aware of what could happen when they are the target of a real cyberattack

Chapter 8 - Conclusion

Since the recent trends show an alarming growth of cyberthreats against the public and private sector, the importance of cybersecurity analyses and frameworks is at an all-time high. Through the interviews, the companies have acknowledged the need for such analyses and frameworks, in order to better protect their data and information. One of the goals this thesis had was to offer clarity regarding analyses and frameworks and gather data regarding their perceived value. In addition, another goal of the thesis was to inform and help raise the awareness of IT companies on which frameworks and cybersecurity analyses are suitable to improve their security. We felt that it was necessary to validate these countermeasures in real life. Due to the fact that we think companies should not blindly trust and utilize analyses and frameworks, since they might not offer sufficient value.

To guide the thesis, and pinpoint exactly what kind of research was desired, three research questions were created. The research questions, combined with the literature review uncovered multiple studies related to the chosen analyses and frameworks. It was still challenging to determine the value of these countermeasures, as no previous study researched specifically that topic. To find new research related to how companies perceive the value of these countermeasures, qualitative interviews were conducted. During the interviews, the companies discussed how they manage their security, but also how they define value related to cybersecurity. The research questions, literature review, qualitative interviews and case studies merged together became the foundation for the findings of this thesis.

Although it is hard to draw any conclusions without more research subjects and data, through this study we discovered various findings. DevelopedIT or small IT companies would most likely benefit from free resources, as they might not have enough resources to invest in cybersecurity at the given time. Albeit medium and large companies would also find free resources such as OWASP valuable. To avoid simple mistakes during development DevelopedIT could look at OWASP top 10 and utilize the guidelines to potentially reduce their monetary loss and time. DevelopedIT, had not given as much thought into their security situation compared to medium and large companies. Through the interviews, we discovered that companies value scalability and flexibility in frameworks. ScandIT especially recommended that other companies look at the NIST framework unrelated to their company size. In order for IT companies to get the most value out of cybersecurity analyses and frameworks, they need to invest based on their threat image and size. All of the companies interviewed as part of this thesis suggested that a company should always outsource security if they cannot do it satisfactory in-house. An important quote from RegionalTech that we would like to highlight is “There is no point in just doing it sloppy. You either do it properly yourself or outsource the task to someone that can deliver a higher quality service”. This quote emphasizes that cybersecurity countermeasures must be taken seriously so that companies do not waste resources such as time and money.

Regarding security frameworks and analyses, they can be used in conjunction in order to supplement each other, so that a company can cover a wider area of concern. All the countermeasures researched in this thesis, were chosen preemptively which was intriguing considering some of the companies interviewed made use of them. This was a positive finding, seeing the countermeasures are well endorsed and widely adopted.

Frameworks make it easier for companies to know which level of security they have and what they want to achieve. In addition, the frameworks also give suggestions on how one should tackle different cybersecurity challenges and how to handle unique vulnerabilities and risks. But technical cybersecurity countermeasures can only protect a limited amount of an IT system. The most crucial part of a system is however the human aspect. All of the respondents confirmed that in order for an IT company to be as secure as possible, it is important to establish an influential security culture. Establishing an adequate security culture can take an extended period of time, nonetheless, both we and the companies interviewed recommended it. A recommendation to how a company can invest when creating a security culture, is through keeping personnel updated on potential security threats or security risks. Additionally, it would be beneficial to also build security awareness through training and mentoring.

References

Accenture Security. (2019). *The Cost of Cybercrime.* Accenture. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Affia, I., Yani, L. P. E., & Aamer, (2019) A. Factors Affecting IoT Adoption in Food Supply Chain Management. Alsetoohy, O. and Ayoun, B. (2018), "Intelligent agent technology: the relationships with hotel food procurement practices and performance", *Journal of Hospitality and Tourism Technology,* Vol. 9 No. 1, pp. 106-120. https://www.researchgate.net/publication/338035901_Factors_Affecting_IoT_Adoption_in_Food_Supply_Chain_Management/citations

Arya Wiradarma, A. A. B., & Arya Sasmita, G. M. (2019). IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company). International Journal of Computer Network & Information Security, 11(12).

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research,* 253(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

Axio. (2020, October). *Top 5 Cybersecurity Frameworks to Secure Your Organization.* Securityboulevard. https://securityboulevard.com/2020/10/top-5-cybersecurity-frameworks-to-secure-your-organization/

Bacudio, A., Yuan, X., Chu, B., & Jones, M. (2011). An Overview of Penetration Testing. International Journal of Network Security & Its Applications, 3, 19–38. https://doi.org/10.5121/ijnsa.2011.3602

Batari, A. (2017). *Web application firewalls: Choosing the right WAF for server security.* Bitninja. https://bitninja.io/blog/web-application-firewalls-choosing-right-waf-server-security/

Cisco. (n,d). *What is Network Monitoring.* Cisco. https://www.cisco.com/c/en/us/solutions/automation/what-is-network-monitoring.html

Cloudflare Inc. (2020). *What is OWASP?.* Cloudflare. https://www.cloudflare.com/en-gb/learning/security/threats/owasp-top-10/

CoreSentinel. (n,d). *Black Box vs. White Box Testing: Key Differences Every organization Should Know.* CoreSentinel. https://www.coresentinel.com/black-box-vs-white-box-testing/

Cuchta, T., Blackwood, B., Devine, T. R., Niichel, R. J., Daniels, K. M., Lutjens, C. H., Maibach, S., & Stephenson, R. J. (2019, 26 September). Human Risk Factors in Cybersecurity. *Conference on Information Technology Education.* 87–92. https://doi.org/10.1145/3349266.3351407

Czechowski, R. (2016). Cybersecurity Risk Analysis and Threat Assessment Within Smart Electrical Power Distribution Grids. *Present Problems of Power System Control*, 7, P. 19-28.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196–207 https://doi.org/10.1016/j.cose.2009.09.002

Garcia, Thea. (2019, October). *What is a Cybersecurity Framework?.* Reciprocitylabs. https://reciprocitylabs.com/resources/what-is-a-cybersecurity-framework/

GeeksforGeeks, (2019). What is cross site scripting (XSS)?. GeeksforGeeks. https://www.geeksforgeeks.org/what-is-cross-site-scripting-xss/

Gerring, J. (2004). What Is a Case Study and What Is It Good for? *The American Political Science Review*, 98(2), 341-354. http://www.jstor.org/stable/4145316

Grant, M. J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. Health information and libraries journal, 26(2), 91–108. https://doi.org/10.1111/j.1471-1842.2009.00848.x

Grassegger, T., & Nedbal, D. (2021). The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. *CENTERIS 2020 - International Conference on ENTERprise Information Systems / ProjMAN 2020 - International Conference on Project MANagement / HCist 2020 - International Conference on Health and Social Care Information Systems and Technologies 2020, CENTERIS/ProjMAN/HCist 2020*, 181, 59–66 https://doi.org/10.1016/j.procs.2021.01.103

Groski, R. (2013, 11 July). How the New OWASP Top 10 2013 Can benefit your business. PivotPoint Security. https://www.pivotpointsecurity.com/blog/owasp-top-10-2013-

benefit-business/

Guru99, (2020). Sql injection tutorial: Learn with example, Guru99 https://www.guru99.com/learn-sql-injection-with-practical-example.html

Höne, K., & Eloff, J. H. P. (2002). Information security policy—What do international information security standards say? *Computers & Security*, 21(5), 402–409. https://doi.org/10.1016/S0167-4048(02)00504-7

Höne, K., & Eloff, J. H. P. (2002). What Makes an Effective Information Security Policy? *Network Security*, 2002(6), 14–16. https://doi.org/10.1016/S1353-4858(02)06011-7

ISO, (2013) *ISO 27001 Structure* [Tabel]. Copied from "Information security management systems - Requirements" by ISO, [2] 2013

Jalkanen, J. (2019). Is human the weakest link in information security?: Systematic literature review. *Information Systems Science.* http://urn.fi/URN:NBN:fi:jyu-201905242795

Keelery, S. (2021, 25 February) *Number of cyber crimes reported across India from 2012 to 2019.* (Cyber Crime & Security) https://www.statista.com/statistics/309435/india-cyber-crime-it-act/#:~:text=Total%20number%20of%20 cyber%20 crimes%20supported%20in%20India%202018&text=From%202012%20to%202018%2C%20there,than%20121%20percent%20since%202016.

Krumay, B., Bernroider, E. W. N., & Walser, R. (2018, November 28). Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework. Nordic Conference on Secure IT Systems.

Lavanya, N., & Malarvizhi, T. (2008). Risk analysis and management: A vital key to effective project management.

Leal, R. (n.d.). *ISO 27001 & ISO 22301 Knowledge base*. https://advisera.com/27001academy/iso-27001-controls/

Lifars. (2020, 24 April). *Injection attacks explained*, Lifars. https://lifars.com/2020/04/injection-attacks-explaine

Lv, B., Yu, X., Xu, G., Yin, Q., & Shi, Z. (2018). *Network traffic monitoring system based on big data technology*. 27–32. https://doi.org/10.1145/3220199.3220221

Mallett, R., Hagen-Zanker, J., Slater, R., & Duvendack, M. (2012). The benefits and challenges of using systematic reviews in international development research. Journal of

Development Effectiveness, 4(3), 445–455. https://doi.org/10.1080/19439342.2012.711342

Mallory. P. (2020, 2 December). *6 benefits of cyber threat modeling*. Infosecinstitute. https://resources.infosecinstitute.com/topic/6-benefits-of-cyber-threat-modeling/

McCabe, J. D. (2007). 9—Security and Privacy Architecture. In J. D. McCabe (Ed.), *Network Analysis, Architecture, and Design (Third Edition)* (pp. 359–383). Morgan Kaufmann https://doi.org/10.1016/B978-012370480-1/50010-4

Mylonas, L. (2020, 19 February). The benefits of OWASP. Codebots. https://codebots.com/application-security/benefits-of-owasp#:~:text=OWASP%20Projects&text=This%20community%20focus%20allows%20the,for%20handling%20their%20private%20data

Nagendrababu, V., Dilokthornsakul, P., Jinatongthai, P., Veettil, S. K., Pulikkotil, S. J., Duncan, H. F., & Dummer, P. M. H. (2020). Glossary for systematic reviews and meta-analyses. International Endodontic Journal, 53(2), 232–249. https://doi.org/10.1111/iej.13217

NIST. (2017, 14 June). *About Nist.* NIST. https://www.nist.gov/about-nist

NIST. (2020, 11 May). *Uses and Benefits of the Framework*. NIST. https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework

NIST. (2020, 15 June). *An Introduction to the Components of the Framework*. NIST. https://www.nist.gov/cyberframework/online-learning/components-framework

NIST. (2020, 23 September). *New to Framework.* NIST. https://www.nist.gov/cyberframework/new-framework

NIST. (2020, 4 June). *Success Stories*. NIST. https://www.nist.gov/cyberframework/success-stories

NMAP. (n.d). *Introduction.* Nmap. https://nmap.org/

Nummikallio, A. (2019). Internet of Things Devices: Case Studies on Security.

Okoli, C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Philosophy & Methodology of Economics EJournal*, 10, 1–51. http://dx.doi.org/10.2139/ssrn.1954824

Othman, S. H. (2017) *ISO 270001 Structure* [Figure], Universiti Teknologi Malaysia. https://people.utm.my/hajar/files/2018/02/Hajar-Lecture-1-Introduction-to-Security-Management.pdf

OWASP. (2017). *Owasp top 10 application security risks.* OWASP. https://owasp.org/www-project-top-ten/2017/Top_1

OWASP. (2017). *OWASP Top Ten*. OWASP. https://owasp.org/www-project-top-ten/

OWASP. (2020). *2020 OWASP Community Survey*. OWASP. https://owasp.org/www-board/attachments/2020-community-survey-v2.pdf

Price, J. H., & Murnan, J. (2004). Research limitations and the necessity of reporting them. *American Journal of Health Education*, 35(2), 66-67. https://doi.org/10.1080/19325037.2004.10603611

Rapid7. (n.d). *What is System Monitoring and Troubleshooting?.* Rapid7. https://www.rapid7.com/fundamentals/system-monitoring-and-troubleshooting/

Raworth, K., Narayan, S., Sweetman, C., Rowlands, J., & Hopkins, A. (2019). Conducting Semi-structured Interviews. *Oxfam GB.*

Renvall, A. (2018). Improving cybersecurity through ISO/IEC 27001 information security standard in the context of SMEs.

Rocha, F. P. D. (2019). *Cybersecurity analysis of a SCADA system under current standards, client requisites, and penetration testing*. https://hdl.handle.net/10216/119066

Saunders MN, Lewis P, Thornhill A, Bristow A. (2015). Understanding research philosophy and approaches to theory development. *In: Saunders MNK, Lewis P, Thornhill A, editors. Research Methods for Business Students.* 7th ed. Harlow: Pearson Education Limited;. p. 122–61.

Sechel, S. (2017). Web Applications *Vulnerability Management using a Quantitative Stochastic Risk Modeling Method* (pp. 16–30).

Splunk. (n.d). *Logging in an app for Splunk Cloud or Splunk Enterprise.* Splunk. https://dev.splunk.com/enterprise/docs/developapps/addsupport/logging/

Splunk. (n.d). What is IT monitoring. Splunk. https://www.splunk.com/en_us/data-insider/what-is-it-monitoring.html

Stiawan, D., Idris, M. Y., Abdullah, A. H., Aljaber, F., & Budiarto, R. (2017). Cyber-Attack Penetration Test and Vulnerability Analysis. *International Journal of Online*

Engineering, 13(1)., 125-132. https://dx.doi.org/10.3991/ijoe.v13i01.6407

Sucuri Guides. (2020, 21 February). *OWASP Top 10 Security Risks & Vulnerabilities.* Sucuri https://sucuri.net/guides/owasp-top-10-security-vulnerabilities-2020/

Tek-Tools. (2020, May). *Network Monitoring: Protocols, Best Practices, and Tools.* Tek-Tools. https://www.tek-tools.com/network/network-monitoring-guide-and-tools

Tunggal, A. T. (2021, 14 May). *How to Perform a Cyber Security Risk Assessment.* Upguard. https://www.upguard.com/blog/cyber-security-risk-assessment

Weisman, S. (2020, 23 July). *What is a distributed denial of serice attack (DDoS) and what can you do about them?*. Norton. https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html

Yin, R. K. (1984). Case study research: Design and methods. *Applied social research methods,* series, *5*. https://www.worldcat.org/title/case-study-research-design-and-methods/oclc/10778402

Zainal, Z. (2007). Case study as a research method. *Jurnal Kemanusiaan, 9*.

Appendix

Appendix 1 - List of questions

1. Who do you think are potential cyberthreats to your company?

a) Potential outcomes of a (threat) on your company

b) Which vulnerable assets in the company do you want to protect from cyberthreats?

c) Which type of attack do you think you are most vulnerable too

d) How would you respond to such an event

e) Do you have a special team to respond to the events (if yes, are they adequate/ efficient, if no, why?)

2. What cybersecurity measures have you implemented for your company?

a) If they have one, are they happy with the one they currently have?

b) If they don't have one, would they be interested in implementing one,

c) Do you have any cybersecurity analysis tools/methods that you wish to follow/adopt or have been adopted by the company?

3. What are your thoughts on cybersecurity frameworks?

a) have you implemented one, why? why not?

4. How do you think that a cybersecurity analysis can benefit your company?

a) Is the cybersecurity analysis financially motivated?

b) Do you consider adopting different cybersecurity measures and policies in order to achieve an ideal security for your company?

c) How would you define value in cybersecurity? (what do you deem as valuable)

5. What would be some reasons to not invest in cybersecurity?

a) Do you have an idea where you should have invested in cybersecurity?

b) Do you have any alternative way to protect your company from cyberthreats, if you choose not to invest in cybersecurity?

6. What kind of data do you want to protect, or do you have any sensitive data on Customers?

Appendix 2 - Contact email sent out to companies

Hei [Company name],

Vi sender denne meldingen fordi det forhåpentligvis er relevant å kontakte dere, i forbindelse med en forskningsrapport ved Universitetet i Agder.

Vi er en gruppe på to som studerer Cybersikkerhet med spesialisering på ledelse. Prosjektet handler om å vurdere verdien av ulike cybersikkerhets analyser og rammeverk for en IT bedrift. Ideen bak forskningsrapporten er at det var et ønske om å få en enklere oversikt over diverse cybersikkerhet analyser. Prosjektet er veiledet av Dr. Jaziar Radianti, og Dr. Marko Niemimaa.

I denne anledningen har vi valgt å utføre intervjuer med IT bedrifter, i forbindelse med vår kvalitative studie. Målet er selvfølgelig å kunne hjelpe oss å samle relevant informasjon, som kan bli brukt til å svare på ulike forskningsspørsmål. Oppsummert handler spørsmålene om sikkerhetsrutiner, deres tanker om trusler, rammeverk, analyser og verdien av cybersikkerhet.

Det hadde vært gledelig å ha et intervju med dere når det passer. Intervjuet vil bli over Zoom eller Teams. Selve intervjuet tar mellom 30-50 minutter, og all data vil selvfølgelig bli helt anonymisert. Dere vil også få et informasjonsskriv som er mer i dybden på hvilke data vi samler og hvordan vi bruker det. Før vi kan ordentlig komme i gang med intervjuet, må vi ha deres signatur og samtykke.

Hvis dere har noen spørsmål angående dato eller retningslinjer på intervjuet, etc. kan dere sende oss en mail på: Andrt15@uia.no Eller Eliasb16@uia.no

Vennlig hilsen,
Andrei Tanase & Elias Burkan