LUND UNIVERSITY
School of Economics and Management

Department of Informatics

The impact of data breaches:

The organizational security measures and the individual perception of an organization's security attempts

Bachelor's thesis 15 hp, course SYSK16 in Information Systems.

Authors: Sarah Shahid
Emelie Huang

Supervisor: Miranda Kajtazi

Correctional teacher: Benjamin Weaver
Umberto Fiaccadori

The impact of data breaches: The organizational security measures and the individual perception of an organization's security attempts

ENGLISH TITLE: The impact of data breaches: The organizational security measures and the individual perception of an organization's security attempts

AUTHORS: Sarah Shahid & Emelie Huang

PUBLISHER: Institution of Informatics, School of Economics and Management, Lund University

EXAMINATOR: Benjamin Weaver & Umberto Fiaccadori

SUBMITTED: August 2020

DOCUMENT TYPE: Bachelor's Thesis

THE NUMBER OF PAGES: 107

ABSTRACT: As people and organizations make themselves more vulnerable on the internet, there is a significant increase in cybersecurity threats. Due to this, organizations and individuals think more about their actions online. However, organizations are constantly improving their methods, when handling confidential data and are developing an understanding of protecting consumers from such exposure. This research has looked into previous literature, regarding the concepts of cybercrime, cybersecurity, and handling of personal data. The empirical data consists of two semi-structured interviews with two individuals working at security departments, within respective organizations. From the interviews, we identified some clear similarities and some that were less obvious. To get a better understanding of the individual perspective, a survey questionnaire was conducted and sent to a mixed group of individuals. The survey results are presented and discussed with the theoretical and empirical findings. The study identifies several conclusions. Including organizational security measures and individuals perceptions of the information provided by organizations, regarding their data handling.

KEYWORDS: cybercrime, information security, cybersecurity, cyber threat, cyber-attack, organization, individual

Table of Content

Tables

Figures

Definitions

Concept	Definition
Cybercrime	Cybercrime is when a criminal makes up or materializes a particular vulnerability or a constant threat for a third party, under a certain financial-economic motivation (Mihaela, 2019).
Cyber-attack	Cyberattacks are the stealing of confidential enterprise data and can be categorized into internal and external attacks (Cheng et al. 2017).
Cybersecurity	Cybersecurity is the ability to protect a cyber environment, and user's assets from attacks (Iguer et al. 2014).
Cyber risk	Cyber risks pose as threats to an organization's information systems, this can lead to loss of consumer and stakeholder confidence (Brockett & Golden, 2012).
Data breach	A data breach is the intentional or inadvertent exposure of confidential information to unauthorized parties (Cheng et al. 2017).
GDPR	General Data Protection Regulation (GDPR) gives EU citizens the rights over their data (Boban, 2018).
Information security (InfoSec)	Information Security is when a company has to protect the flowing information within its departments (Iguer et al. 2014).

1 Introduction

The following introductory sections intend to present a background to the study. Thereafter, the problem area and the research question are presented, which is further concluded by formulating the study's purpose and constraints.

1.1 Background

From a historical point of view, individuals such as employees at companies got access to personal computers during the 1980s, which eventually led to the rise of cybercrime (Oscarsson, 2019). Individuals with good technical knowledge started a movement to perform criminality towards companies. However, the goal of the activity was not always to obtain economic benefits but was to show their knowledge and skills within this area. The aim was to achieve a certain status among others, together with supporting the motto “Hack for fame” (Heickerö, 2012).

According to Verizon's Data Breach Investigation Report (2020), the financial benefit is the key factor behind 86% of the breaches today. Stolen credentials were a major part of the breaches and can be considered a worrying trend according to the report. The situation today emphasizes on the financial factor and how it acts as a driving force for organizations (Verizon, 2020). To put a historical perspective on today, there is a need to understand the shift from “Hack for fame” to “Hack for fortune”. This change began in the late 1990s, and the focus shifted from status and recognition, to the purpose to earn money (Heickerö, 2012; Oscarsson, 2019).

As mentioned previously, data breaching has had a compelling impact on the world of cybersecurity today. According to a report from Gartner (Moore & Keen, 2018), organizations all over the world would spend $124 million on security tools and services. It was an increase of more than 12% from the year before. The amount of resources the organizations have spent that year is still difficult to tell, since there is not much information about it. Overall, these figures indicate that organizations have invested in a lot of resources to secure their systems. Nonetheless, the number of data breaches are still increasing (Moore & Keen 2018). The aftermath of a data breach can be massive and can vary from one organization to another. They can suffer from various negative impacts such as financial losses, scrutiny from customers, and the market, which causes harm to the image and reputation of the organization (Buckman, Hashim, Woutersen & Bockstedt, 2019).

From a practical point of view, in a study made by Accenture (2019), the different consequences caused by cyber-attacks were explored. They identified factors such as, loss of information, loss

of revenue, damages on equipment, and disruption in the business. According to the study, the annual cost on average, as a result of an attack was US$13 million in 2018. The loss of information as an effect was hitting organizations the hardest. With the highest cost at almost US$6 million. Data breaches can be more harmful for an organization's brand image and reputation if customer data is involved. Compared to the leakage of organizational or employee data. The average loss of a brand value is $332 million and to rebuild that image it can take up to one year (Caldwell, 2012).

1.2 Problem area

Since organizations have begun to follow a more digital approach to their business operations. Cyber-attacks threaten organizational innovation, growth, and trust (Culp, 2019). As suggested by Das and Nayak (2013) it is necessary for organizations to take proper measures against cybercrime, in order to maintain consumers' trust and confidence. Organizations do follow certain guidelines and structures concerning the risk management approach. As stressed by Iguer, Medromi, Sayouti, Elhasnaoui and Faris (2014), there is a need for an organizational cybersecurity plan for their systems.

Despite the increase of data breaches and the spending of resources (Moore & Keen, 2018). There is insufficient research available to identify how well cybercrime strategies perform globally. This can for instance be due to lack of interest from cybercrime researchers or a bias in publication (Brewer, de Vel-Palumbo, Hutchings, Holt, Goldsmith & Maimon, 2019). A lack of research about individuals' perception on cybersecurity is also a problem. There is a need for more research to explore the influence on cybersecurity that individuals have (Bishop, Morgan, Asquith, Raywood-Burke, Wedgbury & Jones, 2019). Thompson, McGill and Wang (2017) further added that individuals who use personal computers are not represented enough in security research. It is therefore necessary to explore more about this topic.

The introduction of the GDPR has led to organizations taking security measures for the protection of individuals rights (Boban, 2018). On the other hand, there is limited research about how individuals perceive organizations' outcome when working with this. For that reason it would therefore be essential to make an empirical study on this topic, to gain an insight on the individual's perspective as well.

To summarize, the problems identified are related to the organizational security measures and the limited research within this area. Together with the limited research regarding the individual perspective towards organizational security measures. However, problematizing these challenges is not the intention of this study, but rather to look into the security measures of organizations and how their attempts are perceived by individuals.

1.3 Purpose

The purpose of this study is to describe the organizational security measures and how individuals perceive organizations' security attempts.

1.4 Research question

The challenges mentioned above has lead to the formation of the following research question:

What are the organizational security measures and the individual perception of an organization's security attempts?

1.5 Constraints

The constraints are as followed:

- Interview individuals that work within the security department of an organization.
- The individual aspect does not focus on the psychological view of human behavior such as personal traits or emotions, towards security.
- Survey respondents in this study are considered as someone who has little to some knowledge, regarding cybercrime and cybersecurity.

2 Theoretical Framework

In this study, viewing organizational security measures is essential. Theory wise, we look into security literature to understand how security measures shape organizations. This segment describes the fundamentals of cybercrime, individual behaviour towards security, cybersecurity threats, and preventions. Followed by an explanation of the CIA triad and Task-Technology Fit (TTF) model.

2.2 Cybercrime

For organizations, working with information security went from only being a technical concern for the IT-departments to being important on an organizational level (Oscarsson, 2019). Cyber criminality today is a fully developed, lucrative, and an innovative branch. The ability to earn good money leads to more individuals and organizations working together (Heickerö, 2012). This shows how individuals, together with having the right tools and knowledge, can cause extreme harm to organizations today and to complete these activities, they can even collaborate over borders. The individuals involved can be in different countries when performing such acts. This makes the so-called crime scene global and the risks of being caught have so far been low (Heickerö, 2012).

2.2.1 Consequences of a Cyber-Attack

Every company has an image and reputation and wants to protect it at all cost. Going public with an incident such as a data breach can hit a company hard including its brand image. How the company reacts varies and addressing the news can, therefore, be something a company tries to do with a lot of precautions (Cheng, Liu & Danfeng, 2017; Caldwell, 2012; Ring, 2013). An example of this is Sony, which also owns the gaming brand PlayStation. In 2011, PlayStation Network had personal information including names, addresses, usernames, passwords, etc. stolen by hackers. This affected nearly 77 million of their users, but they did not go public with it immediately. Besides the cost of reputational damages, the European part of Sony got fined by the Information Commissioner's Office (ICO) for not sufficiently preventing the users' information from getting stolen. The fine landed on £250 000 (Ring, 2013).

Today, because of the GDPR, it is mandatory for companies to report the data breaches they are exposed to. After they have a breach, the organization has to report it to the authorities within 72 hours. Those who do not notify would get fines for either up to 2% of an organization's annual revenue or up to €1 million. If an organization does not work according to the law. It can cost the organization up to 4% of the annual worldwide revenue or up to €20 million. This penalty applies to every organization in the EU, and not only organizations that are registered in the union (Ring, 2013; Boban, 2018).

According to the regulations (GDPR), every individual that has been a target of materialistic or non-materialistic damage, due to the violation of the regulations. May be compensated by the personal data controller and personal data assistant (Frydlinger, Edvardsson, Carlström & Beyer, 2018).

2.3 Individual behaviour towards security

The human factor is often described as the weakest link in the security chain (Corradini, 2020; Alqahtani & Kavakli-Thorne, 2019). Human attitudes and behaviour online has proved that despite seeing cybersecurity as something important, individuals do not act according to their attitudes towards cybersecurity (Leukfeldt, 2017). By doing this, individuals increase the potential security risks and put themselves and organizations in a more vulnerable situation. For instance, by handling private information such as passwords inappropriately (Furnell, Khern-am-nuai, Esmael, Yang & Li, 2018). Even though individuals know about the handling of their data, they are not aware of the whole process. However, in terms of protection of personal data, individuals are aware of the importance of protecting it. Nonetheless, they undervalue the risks and consequences of sharing their data and information online (Corradini, 2020).

When it comes to organizations, comprehending the individual characteristics and vulnerabilities, it is considered important for understanding and designing cybersecurity prevention strategies (Corradini, 2020). As mentioned previously by Bishop et al. (2019) more research is needed to explore the influence on cybersecurity strengths and vulnerabilities, due to individual dissimilarities. Thompson et al. (2017) further added that individuals that utilize personal computers are under-represented in security research.

Another important aspect of security is the need for communication to impact individual behaviour and to decrease potential security risks. To be effective, organizations need to communicate at a level that is easily comprehensible for individuals (Corradini, 2020). An example of a common mistake is the lack of policies that are easy to understand when published on organizations' websites (Ooijen & Vrabec, 2019). To be able to contribute with communication, it is necessary for individuals to understand security information that organizations provide. Ideally, the information provided has compliance with the individual's

values and beliefs. Together with motivating the individuals when giving out information on security risks, to succeed (Corradini, 2020).

2.3.1 Individual rights towards their data

Organizations with EU consumers must understand the GDPR agreement (GDPR.EU, 2020). Article 16 of the Treaty on the Functioning of the European Union states that everyone has the right to protected personal data (Frydlinger et al. 2018; Boban, 2018). According to the GDPR, Article 4, the definition of personal data is: "Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." (GDPR.EU, 2020). In other words, personal data is defined by names, emails, social media posts, medical records, etc. Organizations can also collect personal information about a consumer such as gender, race, union, and other unique personal characterizations and are also considered as personal data. However, with the implementation of GDPR, all personal information of an individual will be protected (Cusick, 2018).

An essential part of this is the so-called data controllers that need to take essential technical and organizational measures. By doing this the personal data gathered will be protected and shall not be leaked to unauthorized parties nor be changed or manipulated when unauthorized (Frydlinger et al. 2018). Organizations apply the GDPR implementations and as mentioned in the Information Commissioner's Office (ICO) (2020), GDPR refers to the security principle. It justifies the suitable security of personal data. This includes the protection (technical or organizational measures) against unauthorized processing, accidental loss, destruction, or damage (Information Commissioner's Office, 2020).

2.4 Cybersecurity threats

The leakage of data can be both internal and external. It can either be intentionally through data theft or sabotage by an inside attacker. Or unintentionally through accidental closure of essential information, by employees or partners (Cheng et al. 2017). Today, organizations have been facing data leakage issues to unauthorized parties. Data leakages of any kind can cause harm to organizations in a variety of ways. It can for instance lead to violation of government regulations and in return result in fines and sanctions. This will also affect the organizations', so-called brand reputation, and could lead to a decrease in its sales (Raman, Kayacık & Somayaji, 2011).

There is a need to understand enterprise data leakage threats. As explained by Cheng et al. (2017) intentional data leakages occur because of either external parties or hateful insiders. Data leakage

incidents can be classified into two categories: (1) Intentional threats, (2) Inadvertent and Accidental threats. The external (intentional) threats are in the form of hacking, computer viruses, etc. The internal (intentional) threats would be to commit cyber espionage for some kind of reward or harm because of vengeances. Lastly, there are the internal (unintentional) threats and would be to accidentally publish company data or losing company computers with important data. These are considered mistakes by employees and are a part of the insider threats category as well. The figure below shows these classifications of an insider and external types of threats (Cheng et al. 2017) (See Figure 1).

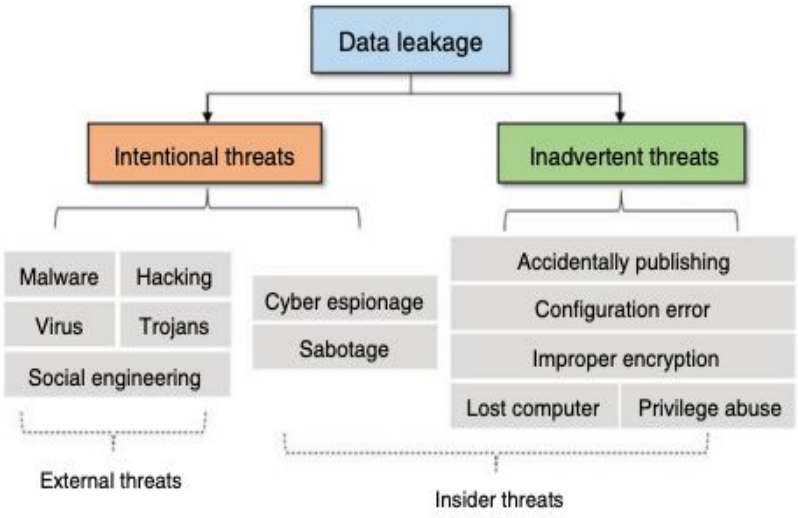


Figure 1: Classification of enterprise data leak threats. (Cheng et al. 2017, p.2)

Iguer et al. (2014) explained through a review by Ernest and Young (EY) in 2013, the focus on the use of information systems within organizations. The review has pointed out some numbers and highlights the increase of internal and external cyber threats. According to the study, 88% report an increase in external threats and 57% report an increase in internal threats. Lastly, 61% note a lack of budget as the major obstacle. To put this into context, they consider internal cyber threats as being a very high-risk factor. The primary source of this high risk is the organization's employees. As they are exploited to sensitive company data and are trusted to a great extent. These individuals can feel that they have the right over company data because they are a part of the research and development of it (Iguer et al. 2014).

To understand the leakage of sensitive data, there is a need to understand that data leakage can occur to an untrusted third party. The factors investigated are the data warehouses and the data

leak channels that are available. It is important to identify the state of the data within the organization because different data states require unconventional approaches (Raman et al. 2011). There are approaches to data leak prevention (DLP) and some current measures that can be taken. One current approach would be to obtain data leak prevention solutions from companies that provide such solutions. Later on, they also mentioned some crucial challenges. In the forms of encryption, access control, and the semantic gap in DLP (Raman et al. 2011; Cheng et al. 2017).

Brockett and Golden (2012) highlighted the increase of cyber threats because of organizations and institutions not being prepared to address and tackle these threats. The article (Brockett & Golden, 2012) explained how the growth of the internet and e-commerce has led to easier access to company data by employees. It further added that there was an increase in threats and financial losses within organizations (public and private sectors). However, by 2008, organizations worked towards tackling these threats and according to the computer security institute, there was a decrease in financial losses. That is mainly because the technology concerning security (software) has improved. Organizations also boosted their internal budgets and were spending more money, time, and manpower to tackle and prevent cyber threats and enforcing laws (Brockett & Golden, 2012).

2.5 Risk management and Data Leak Prevention

As mentioned above this rising concern has led to legislative authorities to become even more active and proficient in this area, which has led to an increase in the number of prosecutions (Heickerö, 2012).

As mentioned above, cyber criminality is an international dilemma and to fight against such crimes institutions need to come together. As Solange Ghernaouti quotes: “Fighting effectively against cybercrime requires a strong political position that brings together public and private bodies and mobilizes them to work together nationally and internationally” (Ghernaouti, 2013, p. 5). Many cyber threats are from another country and it can therefore be difficult to implement laws against these types of international threats (Brockett & Golden, 2012).

A measure against these issues has been brought up by Cheng et al. (2017). The authors explained Data Leak Prevention and Detection (DLPD) as systems that are specially made for dealing with threats and data leakages. Their purposes are to detect by identifying and monitoring, and then to prevent information from getting exposed, intentionally or accidentally. In the article (Cheng et al. 2017), they have two categories for current DLPD techniques, one is appropriate DLPD approaches and the other is basic security measures such as encryption. In DLPD, there is also a content-based analysis and a context-based analysis. With content-based analysis, the organization audits by for instance scanning data to protect it from getting exposed in different states such as rest state, in-use state, etc. It usually manages to get a higher accuracy when detecting, compared to context-based analysis. Organizations have different types of DLPD

systems to tackle different causes of leakage. Detecting internal data leakages can be challenging because insiders know how the organization works and can therefore remove evidence and avoid getting caught and may already have access to sensitive information (Cheng et al. 2017). A part of the detection and prevention is the need for qualified staff within the area. It can for instance be consultants that can aid in outlining potential risks, the financial consequences together with performing and controlling the risk audits, and cyber vulnerabilities (Brockett & Golden, 2012).

2.6 Models

2.6.1 The CIA Triad: guidance for organizational security policies

A model often used in the world of security is the CIA triad which stands for, confidentiality, integrity, and availability. Confidentiality ensures that information is only available and accessible to authorized individuals. Integrity makes sure that data only can be changed in an approved way and that systems can perform without manipulations. Availability ensures that data, services, and systems are available for authorized users (Stallings & Brown, 2018). As the world of technology is constantly changing, there is a need to add new terms into the triad, according to Iguer et al. (2014). The new name would be CIAAA and would include audit and accountability. The audit could help with the improvement of detecting and recovering from attacks and data breaches by auditing the security of events. Holding an employee accountable for their actions by enabling a unique tracking that can trace back to a certain employee (Iguer et al. 2014).

Figure 2: The CIA Triad. (Purcell, 2018)

2.6.2 Task Technology Fit: an organizational tool for evaluation

A model that provides information on the relationship between information security and the work of organizations to assure that regular business activities can continue. Even during an unexpected occurrence called business continuity, as it may help organizations test their overall security (Liggett, 2020). This model, named Task-Technology Fit (TTF), originated from Goodhue and Thompson (1995) who did a study to conduct a research approach in information systems.

TTF can show that technology can affect the performance of a task and its relationship to it, together with the ability of the individual. This means the use of technology (Technology Characteristics box in Figure 3) has to be a suitable match with a user's task (Task Characteristics) for information technology to affect the performance (Performance Impacts). The Task-Technology Fit can also be a tool to help to test, analyze, and diagnose if an information system is satisfying the user and its needs. That is accomplished by breaking down the model, making it more detailed (Hartelt, Wohlfeil & Terzidis, 2015; Shahreki & Nakanishi, 2016). This model was not originally made for security but can be a tool to measure how an organization's information security techniques affect business continuity. Here, the security purpose would be in the Technology Characteristics box and business continuity in the Task Characteristics box. The so-called fit would be the effects (Liggett, 2020).

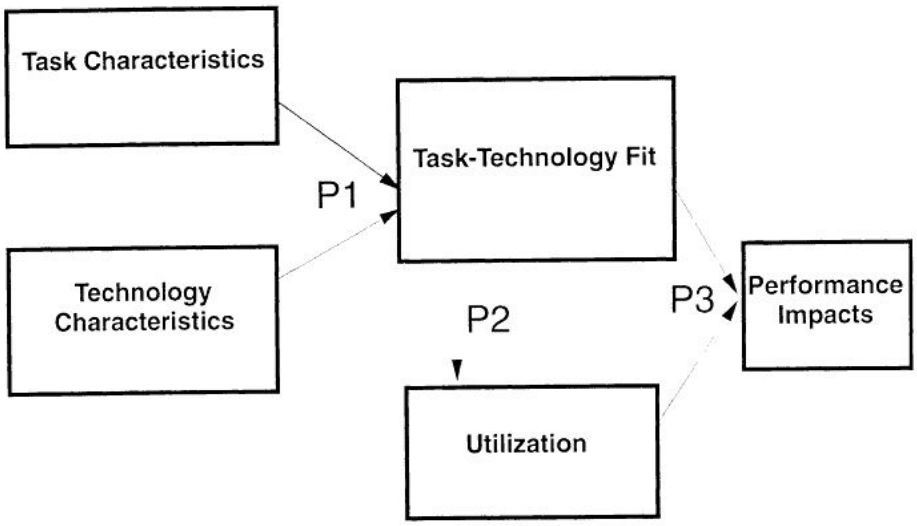


Figure 3: Goodhue and Thompson's Task Technology Fit. (Goodhue & Thompson, 1995, p. 220)

This model was not originally made for security but can be a tool to measure how an organization's information security techniques affect business continuity. Here, the security purpose would be in the Technology Characteristics box and business continuity in the Task Characteristics box. The so-called fit would be the effects (Liggett, 2020).

A measurement of TTF was developed and comprises eight factors, the quality of the data is sufficient for the user and its needs (Quality), having access to correct data (Authorization), finding out the availability and locality of the data (Locality), comparisons and consolidation between data with no disagreement (Compatibility), depending, relying and having access to the systems (Systems reliability), having pre-defined schedules for improvements on production (Production timeliness), how systems understand the task and the users (Relationship with users) and how users use the system and its hardware and software (Ease of use and Training) (Shahreki & Nakanishi, 2016; Liggett, 2020).

2.7 Theoretical conclusion

The purpose of this study is to look into how organizations work to combat cybercrime and the essential security measures taken. Together with how individuals perceive organizational security attempts.

In this research, it is investigated that cybercrime has had an impact on both organizations and individuals. Starting with the organizational aspect, cybercrime has become a concern on organizational level (Oscarsson, 2019). Since such an incident will have an impact on an organization's brand image and reputation (Caldwell, 2012; Ring, 2013). This research presents the prevention of data leakage and how to strengthen the security of an organization, Data Leak Prevention and Detection (DLPD) as it is used specifically as a countermeasure (Cheng et al. 2017). Another common model used within security is the CIA triad standing for confidentiality, integrity, and availability. It ensures that data, services, and systems are available for authorized users and cannot be manipulated (Stallings & Brown, 2018). The study also provides information regarding the use of a TTF model as an evaluation tool for organizations, to measure the fit between their security systems and business continuity. This can be used to evaluate how well their systems work when unexpected events occur (Liggett, 2020).

On the other hand, the individual aspect is more about the behaviour and attitudes towards cybersecurity. In other words, behaviour of individuals can harm themselves and the organizations, since they are considered the weakest link within security (Corradini, 2020; Furnell et al. 2018). The literature describes the current situation of cybercrime and security but

also the human factor concerning individual behaviour and their view on the organization's security attempts.

2.8 Summary of literature

Category	Aspects	Literature
Cybercrime	● Cybercrime ● Cyber-attack ● Consequences	(Oscarsson, 2019); (Heickerö, 2012); (Ring, 2013); (Caldwell, 2012); (Cheng et al. 2017); (Boban, 2018); (Frydlinger et al. 2018);
Individual behaviour towards security	● Cybersecurity ● Human factor ● Behaviour and attitudes	(Corradini, 2020); (Alqahtani & Kavakli-Thorne, 2019); (Leukfeldt, 2017); (Furnell et al. 2018); (Bishop et al. 2019); (Thompson et al.2017); (Ooijen & Vrabec, 2019);
Individual rights towards their data	● GDPR ● Data protection ● Organizations ● Individuals	(Boban, 2018); (Frydlinger et al. 2018); (GDPR.EU, 2020); (Cusick, 2018); (Information Commissioner Office, 2020);
Cybersecurity threats	● Internal and external ● Intentional and unintentional threats	(Brockett & Golden, 2012); (Iguer et al. 2014); (Cheng et al. 2017); (Raman et al. 2011);
Risk management and Data Leak prevention	● Prevention methods ● DLPD ● International collaborations	(Cheng et al, 2017); (Ghernaouti, 2013); (Heickerö, 2012); (Brockett & Golden, 2012);
Models	● TTF model ● CIA Triad ● Evaluation ● Guidance	(Stallings & Brown, 2018); (Liggett, 2020); (Iguer et al. 2014); (Hartelt et al. 2015); (Shareki & Nakanishi, 2016); (Goodhue & Thompson, 1995);

Theoretical conclusion	● Theoretical conclusion	(Oscarsson, 2019); (Caldwell, 2012); (Ring, 2013); (Cheng et al. 2017); (Corradini, 2020); (Furnell, 2018); (Stallings & Brown, 2018); (Liggett, 2020)

Table 1: Summary of literature.

3 Research Method

This chapter discusses the various tools and methods used to gather information for the study and to answer the research question. This section will focus on the research approach, description of the primary data collection process for the interviews, data analysis techniques, ethical considerations, validity and reliability, and lastly reflection of the method.

3.1 Research approach

In this section, we discuss the method selected for the research. The research approach of this study covers some important aspects and the primary focus of research would be to produce knowledge through existing knowledge (Patel & Davidson, 2011).

To explain the conceptual developments, section 3.2 presents methodologically how this is possible. In terms of data collection the *mixed-method research approach* has been applied. This is an approach that collects both qualitative and quantitative data and integrates the two forms of data. The method is used to collect at least one method that collects numbers (quantitative) and one method designed to collect words (qualitative). The purpose of this method is to get breadth, understanding and confirmation. As the research aim is to mix and integrate the two forms of data (Creswell & Clark, 2011). In this research, we collect the qualitative data through two interviews and we collect the quantitative data through one survey questionnaire. We consider it ideal to combine two unique approaches as they can complement each other. Usually, a qualitative approach (interview) applies to get an understanding of the subject. With the help of the results from the qualitative approach, we develop a survey questionnaire (Jacobsen, 2002).

3.2 Data collection methods

3.2.1 Method for developing a theoretical framework

The literature used for the theoretical overview has been analyzed, reviewed, and compared, intending to find new and interesting concepts useful for the empirical study. The table 2 below

shows the themes of each study, followed by the method and the contextualizing of the information value.

Theme	Elements	Literature	Information value
Research methods	Interviews & Surveys and Data collection methods	Forskningsmetodikens grunder, Patel & Davidson (2011) Researching Information System and computing, Oates (2006) Vad, hur och varför? - Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen, Jacobsen (2002)	How to conduct a survey and interview. Important aspects to think about and types of interviews. The difference between Qualitative and Quantitative research approaches.
Security	Information & Cyber security-related threats and historical aspects.	Informationssäkerhet, Oscarsson (2019) Internets Mörka Sidor, Heickerö (2012)	Systematically workaround information security, handling incidents, priorities, and profitability.

GDPR	Introduction to GDPR, and regulations concerning GDPR.	GDPR Juridik, Organisation och säkerhet enligt dataskyddsförordningen, Frydlinger et al. (2018)	Factual knowledge about the various concepts and understanding of how data should be protected and handled.

Table 2: Literature review.

Furthermore, the search engine Google Scholar was used to find articles that tackle these specific topics to show a broader understanding of the specific articles used. We wanted to divide our articles into tables that tackle the different headlines such as threats, cybercrime and cyber security (See Table 3).

Theme	Elements	Literature	Information value
Cyber Crime & Security	Threats	Mihaela (2019) Current security threats in the national and international context	The main focus is to enlighten people about the various threats organizations may face, together with some statistics regarding how much has been prevented in regards to this issue.
	Data Breach	Cheng et al. (2017) Enterprise data breach: causes, challenges, prevention, and future directions	DLPD approaches (Data Leak Prevention and Detection Techniques). Classifications of threats and Enterprise incidents concerning data leakage/data breach.
	Cyber security issues	Iguer et al. (2014) The Impact of Cyber Security issues on Businesses and Governments - A framework for implementing a Cyber Security Plan	This article discusses what countermeasures to take when dealing with cybersecurity issues and threats.

	Risk management	Brockett & Golden (2012) Risk Management for the Future- Theory and Cases Enterprise Cyber Risk Management	This article discusses the potential security risks and how they can be managed. It mentions the difference between internal and external cyber threats within organizations.
GDPR	GDPR on a corporate level	Boban (2018) Cyber Security Foundations For Compliance Within GDPR For Business Information Systems	This study focuses on cybersecurity compliance within GDPR on a corporate level.

Table 3: Google Scholar articles.

The table below shows the searching process for Google Scholar articles used in this study. It also shows the number of hits and the articles we chose for that specific search. To find articles that matched the correct elements and themes of the study, different keywords were made up by brainstorming and were put together in the search bar. Afterward, articles were looked through to find the relevant ones. To narrow down the number of hits, many keywords had to be combined in the search.

Keywords	Number of hits	Chosen article(s)
“cyber criminality” “threats” “security measures” “cybersecurity” “information security” “organizational” “business”	78	Mihaela (2019) Current security threats in the national and international context Iguer et al. (2014) The Impact of Cyber Security issues on Businesses and Governments - A framework for implementing a Cyber Security Plan
“risk management” “organizational” “information security” “cybersecurity” “cybercrime” “cyber risk” “threats” “internal” “external”	403	Brockett & Golden (2012) Risk Management for the Future-Theory and Cases Enterprise Cyber Risk Management
“data breach” “data leakage” “cyberattacks” “organization” “business” “information security” “cybersecurity” “challenges” “detection” “prevention” “strategies” “measures” “internal” “external"	64	Cheng et al. (2017) Enterprise data breach: causes, challenges, prevention, and future directions

“gdpr” “general data protection regulation” “organization” “business” “cybersecurity” “information security” “information systems” “implementation” “compliance” “rights” “protect” “personal data” “personal information”	381	Boban (2018) Cyber Security Foundations For Compliance Within GDPR For Business Information Systems

Table 4: Searching process: Google Scholar articles.

3.2.2 Designing the Interview Guide: from theoretical elements to questions

An interview is not considered a usual conversation because it does not occur by chance. It is rather described as a set of structured questions asked to get specific information about particular issues (Oates, 2006). An interview is a way of collecting information that builds on questions, and there should be a clear purpose of the interview (Patel & Davidson, 2011). The articles used in the sections above are used to plan and develop the research interview questions. The research interview will be semi-structured, which means it will cover a list of themes. However, the interviewer will most likely change the order of questions asked depending on the direction the interview is going. The interviewer might ask supplementary questions if the interviewee brings up topics and issues that the interviewer did not prepare solid questions for (Oates, 2006).

To structure the interview, we have divided the questions into a contract and then different tables with titles concerning a specific issue or theme. We have formulated the questions with the help of the articles concerning the respective topics. This section will explain how the articles listed above have been used for the interview guide questions. The keywords, quotes, and elements are extracted from the articles, and with the help of the keywords, questions are formed. The focus is to choose essential keywords and issues the article proposes and then form simple questions related to the article subject.

The TTF model has also influenced the interview guide. With help from it, three of the eight key factors were used to form three of the interview questions. Those three keywords were: (1) Reliability, (2) Systems Quality, and (3) Authorization. A fourth key factor, (4) Ease of use/Training, can also be considered a part of the (2) Systems Quality factor. To easily identify which of the interview questions were shaped with the help of the keywords, we directly used the words in the interview questions (See Figure 4 below).

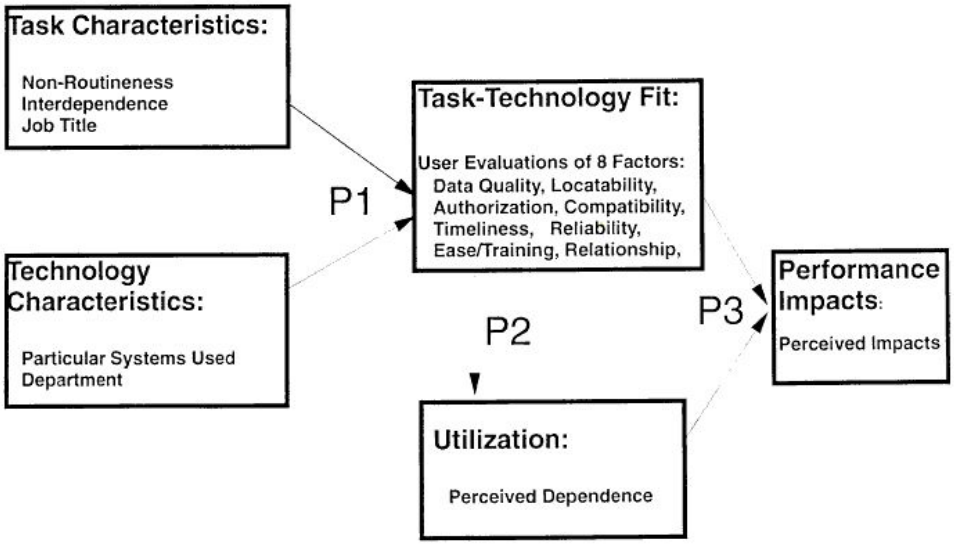


Figure 4: Goodhue and Thompson's Task Technology Fit and the eight key factors (Goodhue & Thompson, 1995, p. 225)

3.2.3 Formation of the Interview Questions

The table below illustrates the key sentences and words extracted from each article to form interview questions for the interview guide.

Author & Article	**Key terms**	**The Interview Questions**	**Appendix**
Mihaela (2019) Current security threats in the national and international context	● Cybercrime ● Cybersecurity	1. What does Cyber Crime entail for you? What does Cyber Security entail for you?	Appendix 1

Brockett & Golden (2012) Enterprise Cyber Risk Management	● Internal cyber risks ● External cyber risks ● Cyber- threats (Financial) ● Risk management processes ● Mitigate cyber threats.	2. Does your organization separate the risk types into categories? a. Such as Internal and External risks, and if so, how are these managed? b. What are the financial effects of Cyber-threats and the risks that follow? 3. Does your organization have a Risk Management Process tailored to: a. Mitigate and control Cyber-threats?	Appendix 1
Cheng et al. (2017) Enterprise data breach: causes, challenges, prevention, and future directions	● Data breach ● Confidential information ● Unauthorized parties.	4. What do you know about the term Data Breaching?	Appendix 1
Iguer et al. (2014) The Impact of Cyber Security issues on Businesses and Governments - A framework for implementing a Cyber Security Plan	● Cybersecurity ● Data breaches	5. How would a Data Breach affect your organization? a. Financially? b. Reputation and Brand image? From a customer's perspective and an employee's perspective?	Appendix 1

	• DLPD approaches: *Data Leak Prevention and Detection Techniques*	6. How does the GDPR affect the way your organization works with detection, prevention and announcing a Data Breach?	Appendix 1
	• Cybersecurity plan • Countermeasure information leakage • External or internal, intentionally or unintentionally.	7. Could you explain what plan or strategy(s) your organization has developed to combat Cyber Crime and prevent Cyber-attacks such as a. Data Breaches?	Appendix 1
	• Customer data • Employee data	8. Has your organization had any Data Breach, external or internal (as a direct effect from your mitigation plan or strategy)? 9. How does your organization tackle threats and challenges, such as? a. Data Breaches? 10. Are there any issue(s) that cannot be solved before a Data Breach has occurred? a. What proactive measures are taken?	Appendix 1

Boban (2018) Cyber Security Foundations For Compliance Within GDPR For Business Information Systems	• GDPR strengthen existing rights • Individuals control over personal data.	11. How does your organization work with GDPR? a. How does your organization manage the personal data and information of your *employees*? b. How does your organization manage the personal data and information of your *customers*? 12. What were the key factors in your organization focused on when getting ready for the GDPR implementation?	Appendix 1
	• Protect citizens in the EU from data breaches. • Protect and empower EU citizens with data privacy. • Pressure on businesses and their information systems- increase cybersecurity (challenge)	13. Since introducing GDPR in 2018, what has changed in the way your organization handles data and information from: a. Employees b. Customers 14. Is there any current challenge(s) that your organization has to deal with concerning GDPR? a. Regarding the implementations of the new GDPR laws? 15. Any previous challenge(s)? Possible future challenge(s)?	Appendix 1

Table 5: Formation of interview questions.

3.3 Interviews

3.3.1 Selection of interviewees

Before contacting organizations for interviews, we wanted to determine some criteria for our potential interviewees. After we set the criteria, we identified key organizations fulfilling those requirements. To contact the organizations, we took the help of our supervisor, Miranda Kajtazi, who knew individuals that worked at the first organization (organization 1) and that provided us with the contact of interviewee 1. The contact to interviewee 2 (organisation 2) was provided to us by interviewee 1.

The criteria identified were:

- **Part of the security (Information or Cybersecurity department) -** The aim was to interview individuals who have experience within this field. Mainly to generate specific answers regarding the security environment in their respective organizations.

- **Some knowledge about GDPR and its implementation -** There was a requirement that the interviewees have some kind of GDPR knowledge so they can respond to GDPR specific questions.

- **Individuals from different companies -** Last, there was a need for variation and we sought individuals from different companies. This also provided the research with unique aspects concerning the topic and issue.

Organization	Name Anonymous	Role/Title	Type of interview	Date and time	Interview length	Recorded
Organization 1	Interviewee 1	Reporting manager, within security	Video call (Microsoft Teams)	Part 1: April 6th, 2020, 10.00 - 11.00 Part 2: April 14th, 2020, 15.30-16.30	Part 1: 1 h Part 2: 1 h	Yes
Organization 2	Interviewee 2	Group Information Security Officer	Video call (Microsoft Teams)	April 28th, 2020, 15.00-16.20	Approx. 1 h, 20 min	No

Table 6: Selection of interviewees.

3.3.2 The interview scenario

We discussed that having an interview in person would make it easier for us if we would be closer to the meeting place. At the same time, we knew that it might limit the selection of interviewees to only within a limited area. Due to the current pandemic, we also knew that the chance of meeting in person would be small. So, to make everything easier for all parties and to have the opportunity to contact someone outside our geographical boundary, the interviews were conducted online. Both were done on Microsoft Teams, which went well. However, a problem that can arise when the interviews are done in this way, is the lack of personal contact. As interviewees can speak more freely when interviews are conducted in person (Jacobsen, 2002).

3.4 Designing the survey: from theoretical elements to questions

When conducting a survey there is a need to understand what the purpose of a survey is. The fundamental purpose would be to get data from a large group of people in a more standardized and systematic way. This data is used to look for patterns that can be generalized to a larger population, compared to the group that was targeted in the survey (Oates, 2006).

3.4.1 Formation and publication of the Survey Questions

For this research, a survey via a questionnaire was conducted and when designing it we kept some key factors in mind. As mentioned by Oates (2006), there is a need to decide what data requirements there are and that the data generated is associated with the research questions. If it is (1) Directly topic-related and focuses on the specific question. Or if it is (2) Indirectly topic related and ask indirect questions that are related to the topic such as age and gender. In our survey we have applied both the direct and indirect topic-related questions.

We formed the survey questions based on the interview guide. The questions had to be comprehensible for participating individuals, who may not have much knowledge of the topics of this study. The questions in the survey will focus on the rights of individuals concerning GDPR and their knowledge of cybercrime. By doing this, the research will generate data based on an individualistic approach.

Table 7 below illustrates the transformation of interview questions into survey questions. We have separated the interview and survey questions into columns, and the third column "Comparison" shows what is attained by the interview and survey questions. As shown, the interview questions (Interview Q) are focusing on the organizational aspect, hence the questions are more specific. Whereas, the survey questions (Survey Q) are considered more general and do not require a specific answer. Since they mostly are Yes or No questions.

We designed the survey with a front-page with information about the research issues, a segment with definitions of terms used. The survey was created with the help of the software tool (Survey Monkey). The goal was to make a fairly short survey questionnaire with approx. 8-10 questions. The complete survey guide can be found in (Appendix 2).

Interview questions	Survey questions	Comparison
1. What do you know about the term Data Breaching?	1. Are you aware of Data Breaching (leakage) issues within organizations?	***Interview Q1****:* Elaborate on the term from an organizational view. ***Survey Q1****:* Is there any knowledge about the term?
2. How would a Data Breach affect your organization? a. Financially? b. Reputation and Brand image? From a customer's perspective and the employee's perspective?	2. If yes, which of the following data breaching(leakage) issues concerns you the most: (rank them in order of most concern): Stolen identity information, Stolen credentials, username/password, stolen credit card details	***Interview Q2****:* The effect on the organization's overall reputation, what happens? ***Survey Q2****:* What are normal individuals more concerned about when there is a leakage (focusing on their data leakage)?
3. Technology is constantly changing, what does your organization do to keep your System's Quality high together with keeping employees and customers up to date?	3. If yes, which data handling procedure would make you feel the safest: a. Outsourced data to a third party with a known reputation b. In-house data handling with the latest technology	***Interview Q3****:* Technical question regarding the organization's work within this area. ***Survey Q3****:* About the preference of an everyday individual concerning the technical aspect of an organization (Data handling).
4. From a technological and a software point of view, can you elaborate on the technical reliability within the organization?	4. To what extent are you concerned that your data can be leaked due to for instance cyber attack(s) or technological errors within organizations? 1-5 (scale)	***Interview Q4****:* Technical question concerning reliability to get a more specific answer. ***Survey Q4****:* Concern amongst individuals regarding technological errors and cyber-attacks.

5. How does your organization work to ensure that your customers are aware of the organization authorizing their data?	5. Have you ever thought about how your data is being handled by organizations?	***Interview Q5****:* Find out how organizations reach out to their customers. ***Survey Q5****:* Investigate if individuals worry about their data and its handling.
6. Since the introduction of GDPR in 2018, what has changed in the way your organization handles data and information from: a. Employees b. Customers	6. GDPR is often referred to as the strongest regulation ever created. Do you know what capability GDPR has to protect you?	***Interview Q6****:* Organizational overview of any key differences since GDPR ***Survey Q6****:* Individual's knowledge of GDPR.

Table 7: Formation of survey questions.

3.4.2 Selection of survey participants

When selecting the survey participants the survey questionnaire was sent through social media platforms, more specifically Facebook and Linkedin. Since this survey addresses an issue that concerns a mixed group of individuals, we wanted to send it to people that we believe have little to some sort of knowledge regarding this subject. Since we reached out to a narrow group of individuals, the responses might have an affect on the overall survey results. It is also important to take into consideration that the participants do not have a correlation with the organizations interviewed. In this case, the survey questionnaire was sent to individuals that were a mix of students studying information systems, business, and IT-related subjects and employed. However, it might be considered biased to send out the survey questionnaire to some individuals that might have some knowledge about the topic. Therefore, the sample of survey participants can be considered restricted and might not describe a broad cross-section of the general population (Gravetter & Forzano, 2009).

3.5 Ethical considerations

An email was sent to both interviewees with an invitation to participate in our interview. Together with a presentation of our research question, purpose, interview contract and the questions. Both interviewees replied to our request positively and Microsoft Teams meetings were scheduled respectively.

3.5.1 Recording and transcribing

Each interview begins with the interview guide's introductory part (contract). The section is the consent of the interviewer regarding the recording and transcription of the interview. Interviewee 1 approved the recording of the interview and subsequent transcription. Whereas, Interviewee 2 did not approve of any recording of the interview, since it goes against the organization's guidelines. However, note-taking was acceptable when interviewing the individual.

3.5.2 Anonymity

A question was asked about whether the interviewees wanted to be anonymous, or if we could mention their and their company name in the study. Both interviewees did not agree to the mentioning of their name nor the company name. The individuals made clear that the study should not mention keywords and terms specific to the organizations, as it can easily be referred back to.

3.6 Data processing

3.6.1 Interview Transcription and Interview Notes

After completing interview 1, the interview recording was transcribed by one of the researchers and can be found in the appendices. The interview was conducted in Swedish and the transcript was not translated, since the aim was to present the original quotes and terms said by the interviewees. However, the quotes have been translated to English in the actual text to make it easier for the reader to comprehend the information. When transcribing the interview we decided to remove repetitions and unclear sounds, to make the transcription more readable. The transcript

was controlled by the other researcher who had not worked with the transcription. Any occurring spelling errors, sentence constructions, or confusing phrases were discussed and corrected.

Interview 2 was also conducted in Swedish but since interviewee 2 did not allow us to record we actively took notes during the interview. Both of us took notes and later compiled them. The notes were used as a basis for the interview and can be found in the appendices as well. Some of the quotes used from the interview in the actual text have been translated to English.

After transcribing interview 1 and compiling the notes from interview 2, we gathered the information to discuss how we perceived it and outlined the parts necessary for our research. Later, the most relevant information was selected and discussed in the discussion chapter.

3.6.2 Analyzing the survey data

The survey and the interviews were meant to complement each other since both the interviews and the survey provides the research with essential information. The survey data has been looked into with the help of an online survey software, SurveyMonkey. After we got enough responses, we closed the survey to start analyzing the data. The previously mentioned software made it possible to create a pie chart out of the survey results and made it easier for us to read and analyze the data as a whole. To get a more in-depth understanding of the results we went through every single answer separately. After going through all of the results, we discussed and selected the most relevant responses and presented them in the empirical findings and discussion chapter.

3.7 Research Quality

3.7.1 Validity

A part of the research quality is the validity of the research arguments, which means that the conclusions drawn from the data are sensible to follow (Sapsford, 2007). Throughout the method chapter we have discussed the validity of the methods applied. The consequences concerning the different methodological approaches, have been discussed in this chapter. Our empirical research is limited to a few respondents and this should be taken into consideration. Since the conclusions should not be seen as facts but rather as guidelines.

3.7.2 Reliability

According to Jacobsen (2002), reliability is a term used to describe credibility. The interviewees were therefore carefully selected to that extent that both of them work in the security department.

We also wanted to interview individuals who had a lot of experience in the field of cyber security. Based on this, the interviewees are considered relevant and knowledgeable within the subject and can contribute with essential knowledge and information to help us answer our research question.

Prior to the interviews we had clearly explained the research aim. The research purpose together with the interview questions were gathered in a document and sent out to the respective interviewees. We also followed an interview guide, which means the interviews were based on the same questions.

Another way of checking the reliability is to use more than one factor and study their results (Sapsford, 2007). We have done this by conducting a survey questionnaire and sent it out to a total of 67 participants and later presented and discussed the results. By doing this we have collected information from more than one individual, to get an individualistic perspective.

3.8 Reflection of method

Since the research has used a mixed-method approach which means that both qualitative and quantitative methods have been applied. The combination of both methods can be considered ideal (Jacobsen, 2002). However, there are advantages and disadvantages with respective methods and that have been taken into consideration in this research.

The qualitative advantages would be the focus on the details, nuances and picking up something unique with each respondent, as you get different opinions from the partaking individuals (Jacobsen, 2002). When we were looking through the interview recording, we observed the fact that we got some individual aspects and experiences from the interviewee. Even though the questions were targeted towards the organization, we did get answers relating to the respondents and their personal views. As there are advantages there are disadvantages. In this case, the main disadvantage would be the respondents need to overshare their experiences and thoughts for a specific question. This could sometimes become overwhelming as it was a lot of information to grasp, which felt like a never-ending vicious cycle (Jacobsen, 2002). Another disadvantage is the fact that it is resource-intensive, to conduct interviews. Due to it being time-consuming and difficult to get many respondents partaking in an interview (Jacobsen, 2002).

We believe that this research could have been improved if there were more interviews as it could provide the research with more representatives concerning this topic. As mentioned by Brinkmann (2013, pp. 144-145), “Qualitative studies cannot, like quantitative studies, demonstrate generalizability statistically”. In other words, conducting interviews may not give a generalized view of the subject investigated and can therefore be considered subjective.

In conclusion, we have explained the methods used in this research and identified their validity and reliability. As a part of the method reflection we have highlighted the advantages and disadvantages of the qualitative approach and also mentioned the possible improvements.

4 Empirical findings

In this section, the findings from the interviews and survey are gathered and presented. The answers from the interviews are summarized and the main themes of the respective interviews are highlighted. The interview transcriptions and the survey results will be presented in the appendices.

4.1 Presentation of the Interviewees

Direct quotations from the transcript are cited in the following manner: Int1:51 refers to Interviewee 1, line 51.

Interviewee 1
Interviewee 1 has over 20 years of experience in information security and cybersecurity. The individual has worked with questions regarding cybersecurity and IT- security, related to infrastructure, applications, and tactical and strategic questions (Int 1:33). Interviewee 1 has previously worked as a consultant, in different companies and projects within information security, cybersecurity, and payments and is now working with information security at organization 1 as a reporting manager (Int 1:26, 28). The interviewee's role is about visualizing where the organization stands, its current state regarding information security and data privacy (Int 1:28). Together with making sure they follow up on their demands and requirements on the implementations (Int 1:45). The current state of security, the current state of privacy, risks, and any positive trends will be reported to the organization's management board (Int 1:28). The interviewee has three main responsibilities that are to build the reporting capability, contribute to projects and to ensure the implementations of the processes and capabilities the organization sets up (Int 1:51).

Interviewee 2
Interviewee 2 works as an Information Security Officer (ISO) today and is responsible for reporting to the Chief Information Officer (CIO) (Int 2:16). Currently, the individual is working within the Corporate security department, with management systems for information security. The role is to build the management systems for security and work within a wide range of security areas (Int 2:22). Previously, the interviewee worked as a DPO (Data Protection Officer) for a year focusing on GDPR related tasks within the same organization (Int 2:18, 22). The

individual has a background in revision and IT- management consulting within the field of information security (Int 2:20). A typical workday varies a lot for the individual, as it is not considered a regular 8-16 job. The individual explained the job as not being repetitive, which means that they do not do the same thing every day. Usually, they do projects and have flexible working days (Int 2:26). As a whole, the organization is organized into six different areas with different criteria on security. There are millions of customers which means that there is a significant amount of personal data that needs to be protected by the organization (Int 2:24).

4.2 Cyber threats and risk management

Interviewee 1 explains the so-called "risk universe" of the organization and how it is divided into different sections. The organization (1) revise and update their risk universe and base them on known and well-adapted frameworks. Regardless of how far they have come with it, the risks are divided into different categories. For instance strategic risks, social risks, financial risks, compliance, and technological risks. However, not so many internal and external risks. The interviewee (1) describes that information security is not a category on its own. As it is considered a part of the technology risks but also all the other risk categories, cyber specific risks are mostly under the technology category (Int 1:66). According to interviewee 1, the type of risks depends on the person you are talking to. For some people, it is about the impacts and probability, and for others, it is more about threats and vulnerabilities, but all four define risks (Int 1:86-87).

The interviewee (1) also explains the specific processes to tackle and control cyber threats. There is a risk management process where they handle cyber security, digital security etc. (Int 1:85). The organization's internal framework is considered responsible for the implementation of rules and regulations used to tackle risks. The individual stresses on two types of risk management techniques. The first approach is when the organization knows what type of risks there are to be addressed and that easily can be tackled. On the other hand, there is a process to make an impact assessment of the potential risks and then classify them. Then they will get a classification of relevant measures and will know how to apply it to that specific risk (Int 1:88).

Interviewee 2 talks about the processes concerning security and that it should be systematic and risk-based. As quoted:

"*Yes, one of the basic principles is that it must be risk-based. Risk analysis is fundamental.*" (Int 2:30)

Further, the individual elaborates on various strategies when trying to combat cybercrime. There is a need to understand who the criminals are and monitor potential threats.

"(...) monitor the surroundings and have contact with authorities, what threats we should search after for instance, Russians, Chinese and what our Security Operation Center (SOC) should keep an eye on. Knowing your opponent is an important strategy." (Int 2:43)

Interviewee 2 also emphasizes the educational and recruiting aspect when tackling cyber threats. The individual believes that it is tough to find qualified staff within this field. The interviewee elaborates on the purpose to identify the threats and the challenges related to them. For that reason, there is a need for competence that understands these issues (Int 2:46).

4.3 Detection, prevention, and, announcement

As described by interviewee 2, there is a requirement of acting and reporting a data breach within 22 hours. There is also a need to announce the incident to the employees, to create awareness of the issue. Even the slightest suspicion of a breach should be reported to the right person within the organization. The announcement does have an impact on the organization (Int 2:41). Even interviewee 1 mentioned that they have routines for communicating with their employees if information leaks out (Int 1:135). Organization (1) ensures that all routines and processes are in place and that they work according to the law (Int 1:161).

"There are routines of communication with the affected, when personal information has been leaked, whether they are customers or employees, together with the authorities of course. Since we have an obligation to report." (Int 1:137)

Nonetheless, both interviewee 1 and 2 talked about the risk management regarding financial aspects. As quoted below:

"Yes, it is a very difficult question to answer (...) There is a big impact on our business if it would be exposed to data leakage or fines from the authorities. If it would have been a crucial leakage of personal information, personal data then the penalty would be quite high in relation to our turnover internationally (...)" (Int 1:73)

"It is difficult to put a price tag and be precise when it comes to risk management. But it is only guesses at the end of the day. Organizations with intrusion have had an impact on their share, but it usually goes up again (...) there are definitely financial costs." (Int 2:33)

Interviewee 1 mentioned that besides the financial impacts, data leakages can also impact the brand image, their reputation and the social aspect (Int 1:79, 120). Interviewee 2 talked about

how leakages can affect the public's view on the organization as it could affect the brand and reputation of the organization (Int 2:34).

As a part of the prevention process, organization 2 has a group that works with the first line of defense and security related questions. Regarding data breach within the definition of GDPR, interviewee 2 explains that a lot of people work within that area and that it is prioritized (Int 2:47). The interviewee (2) elaborates on how prevention makes sure that the organization works systematically with information security. The detection prospects are to monitor and strengthen their work with their Security Operations Center (SOC) (Int 2:41). Interviewee 1 talks about detection as something that is about monitoring and following up. Together with prevention and reaction that is about response and a bit about intelligence (Int 1:36).

Something else organization 2 works with is to educate their employees in a more playful way and teach them more about security related issues. This has been done through e-learning, lectures, sending out articles in the organization's intranet, and testing them. It is important to create awareness amongst them since they are a big source of risk as they are capable of making mistakes. The focus is to work continuously with the employees (Int 2:39). On the other hand, they are also communicating with their customers and making sure their data is secure. It is done by making sure that they do not share their information with anyone else, and to change passwords every so often (Int 2:40). According to interviewee 1 more than half of all attacks that occur are due to insiders (Int 1:62).

4.4 The technological approaches

Interviewee 2 also talked about some of the technological approaches. The organization conducts risk analysis on more sensitive systems. Such systems should have a higher demand for passwords and fingerprints. Since there is a requirement on security when installing new systems, it is important to do a risk analysis to make sure that the right system has been installed. So, if a system has sensitive information, it should have higher safety requirements such as passwords, fingerprints, etc. (Int 2:37). Another approach to the technological challenges is the incorporation of the GDPR. Since it is important to balance the use of technology and the laws and regulations of the GDPR. For example, an organization would find it helpful to be able to track logs to investigate a data breach. Interviewee 2 further added that one should be careful to not cross the lines of privacy (Int 2:55).

Interviewee 1 described the technological approach as being about the organization's applications and the supporting infrastructure. The individual highlights how the application's criticality is measured based on three different aspects of a CIA triad. That is confidentiality, integrity, and availability. With the help of this, they can classify the criticality of that solution and the

requirements needed for that application (Int 1:124). Interviewee 1 does elaborate on the use of the triad within the organization. The individual talks about the controls or system requirements used to form the applications or products. These so-called controls include the fundamentals of the CIA triad i.e. confidentiality, integrity, and availability and are therefore used in the classification process (Int 1:124-125).

The interviewees also talked about the outsourcing of data to third parties. Interviewee 1 mentioned the third party security management from a strategic aspect. It is about having as much control over the outsourced data as in-house data (Int 1:143). The outsourcing of customer data is mentioned by interviewee 2, and the importance of making sure the contractors dealing with the data knows their obligations (Int 2:52).

Further, interviewee 2 mentioned that there should be a need to implement a new security system. As the individual emphasized that technology is important but it can not solve all problems.

"(...)There must be a need to provide security and similar products and systems, not just that someone says it's good and that it's "trendy". Technology is very important, but one can think that technology can solve all problems, but if you cannot interpret or show the result, you do not have much advantage from it. There must be a need for a system." (Int 2:45)

4.5 Authorization of data and awareness

Interviewee 1 elaborates on their working routines and processes and how they divide the work. As they make assessments, audits, and make sure that all the applications and products with personal data are identified.

"Some work proactively with monitoring and so on. Some work reactively with incident response for instance. And others work with assessments where they do audits, mapping and their role is to ensure that we identify all of our products, applications that process personal information. If it is about employees or if it is about customers." (Int 1:160)

The interviewee 1 further adds that there are technical security measures such as encryption and controls implemented to prevent a data breach. With all this in place, the organization has a relatively good overview of what applications need to be used to process personal data of both employees and customers (Int 1:161).

Interviewee 2 talks about the unity between information security and data protection and that they should not be considered separate projects.

"GDPR implies both legal aspects and technical aspects and you should be able to handle both." (Int 2:48)

Both interviewees talk about communicating with their customers. Interviewee 1 elaborates on a more technical approach. Where the organization communicates through the latest version of applications including, mobile apps and websites (Int 1:163). It is a useful way of communicating the rights and the obligations of the consumers and what we do with their data (Int 1:132). This in return leads to a continuous dialogue about customers and their data, as quoted:

"(...) but we do not sell data to anyone and we only share data with our partners who possibly help with specific tasks. And we are very careful and communicate about it as well." (Int 1:164)

Even interviewee 2 explains the importance of making the privacy policies available for customers. Together with making them comprehensible, since it is necessary to look at the situation from a customer perspective. Therefore, it could be helpful for the customers if the organizations would not post long paragraphs with essential information (Int 2:51). Organization (2) emphasized on the communication with subcontractors and them knowing their obligations (Int 2:53).

The interviewees also mentioned the positive effects of the GDPR implementation. As it has developed a culture that is more aware of how to handle security-related issues. Nowadays, workers are more afraid of making mistakes because of new rules and regulations.

"(...) GDPR had a positive effect on the entire security work, and made employees more aware of security risks. A culture that is much more aware, they are much more aware of how they should manage information (...)" (Int 2:54)

"Above all, it has also created a great deal of fear, fear of making mistakes, which means that there have been a lot of questions from the organization about how to react in certain situations and so on, because individuals do not want to make any mistakes and do not want to expose the company and the brand unnecessarily. So, there are very positive effects of the law of GDPR." (Int 1:168)

4.6 Prospects

Regarding future challenges, the interviewee 2 described the process of security handling and data protection as continuous and challenging. The individual also thinks that it is essential to develop processes continuously as a part of the overall process (Int 2:58).

Interviewee 1 focuses on the digital aspect and believes that the bigger challenges are to migrate to more developed applications and decommission older applications (Int 1:171-172). Another challenge is to have complete information about where customer data is permissible to be stored. To put the challenge into context, it could for instance be to store customer data in another country or continent (Int 1:93).

Interviewee 2 elaborates on the GDPR aspect as one of the future challenges. The individual emphasized on the fact that the different legislations in different countries lead to various interpretations of the regulation. For instance, there can be different versions of the same regulation in Germany when compared to Sweden. This poses a challenge, but the individual believes that it is something that should be followed up and worked with for the functioning of the organization (Int 2:57).

4.7 Presentation of survey results

4.7.1 Gender, age, and, occupation

The survey questionnaire got a total of 67 responses that consisted of 30 females, 35 males and 2 others. 33 individuals belong to the age group of 16-25 years and 18 of the respondents in that group are females, 13 respondents are males and 2 respondents are others. A total of 33 individuals belong to the 29-49 age group. In that group, 21 were males and 12 were females. Whereas the 50-65 age group consisted of 1 male and no respondents in the over 65 age group.

A majority of the respondents are employed (approx 48%), the second most are students (approx 37%), a fairly small group are unemployed (approx 5 %). Lastly, we have others e.g. someone who is a student and employed (approx 10%).

4.7.2 Awareness of the issue

Regarding the awareness of data breach (leak) issues. 50 individuals answered *Yes* (approx. 75%), a quite small group of 7 individuals answered *No* (approx. 10%) and 10 individuals answered *Not sure* (approx. 15%). 58 out of 67 participants considered stolen credit card essentials as the biggest concern (approx. 41%), 35% ranked it as the second biggest concern and 24% ranked it third. Further, the stolen identity concern was ranked number one by approx 38%, at number two by 36% and at third place by 26%, of the participants who answered. Lastly, we have the stolen password and username concern, where 21% of the individuals ranked it at first place, 29% at second and 50% ranked it at third place.

4.7.3 Concerns regarding Data Leakage

A question about data authorization was asked and if they have ever thought about how their data is being handled by organizations. A total of 31 out of 67 participants answered *Yes* (approx. 46%). 29 answered *Sometimes* (approx. 43%) and only 7 individuals answered *No* (approx. 11 %). No one answered *Not sure.* The answers regarding the safest organizational data handling method showed what the participants preferred. Out of the 59 that answered this question, 44 individuals (approx. 75%) chose the in-house data handling with the latest technology as the safest procedure. The rest, which consisted of 15 individuals (approx. 25 %), chose the outsourced data to a third party with a known reputation. The survey also measured the concern rate amongst the participants, regarding data leakage due to for instance, technological errors made by organizations. Out of all the 67 participants that answered this question, an average of 51 was shown on the diagram.

4.7.4 Data Authorization and GDPR

The second last question of the survey questionnaire is about individuals' knowledge about GDPR and its capability to protect them. According to the results, a vast majority of approximately 67% (45 individuals) answered *Yes.* A quite small group of 8 individuals (approx. 12 %) answered *No* and 14 individuals answered *Not sure* (approx 21. %). The last question is about how well organizations communicate with their customers, more specifically regarding the handling of their data. Basically, if individuals think that organizations handling their data gives them enough information about it. In this case, 7 individuals answered *Yes* to this question (approx. 10%), whereas a small group of 4 answered *Not sure* (approx. 6%). The majority answered *Sometimes,* which consist of a total of 36 individuals (approx. 54 %) and 20 individuals answered *No* (approx. 30 %).

5 Discussion

This chapter discusses and compares the empirical findings with the theoretical framework to identify similarities and differences. The results from the survey are also discussed and compared in this chapter. The discussion has some of the same headings as the empirical findings chapter to easier make connections between the topics.

5.1 Cyber threats and risk management

The results from the interviews indicate that working with risks is a major part of the organizations' strategies. Whilst interviewee 2 highlighted that working risk-based is fundamental to the organization. Interviewee 1 went more into detail about the types of risks and who you are communicating the risks with. For example, when communicating with business stakeholders, the risks will be more about impact and probability. Whereas for technical stakeholders it will be more about threats and vulnerabilities.

Both interviewees talked about how they monitor logs, controls, and systems to find vulnerabilities. Also how they identify risks, potential threats, and vulnerabilities. This was also brought up by Brockett and Golden (2012) who highlighted monitoring and detecting as essential when mitigating risks. Having qualified staff within this area is also important according to Brockett and Golden (2012) and interviewee 2. However, interviewee 2 mentioned the difficulty to find qualified individuals. Whereas interviewee 1 does not talk about the importance of this aspect. This shows that identifying and keeping track of potential risks is necessary when working with security. Together with finding qualified staff, even though it can pose as a challenge for some organizations.

As well in the case of internal and external risks, we were able to spot differences in the work of organization 1 and 2. For example, interviewee 1 mentioned that they do not categorize their risks into external and internal risks but talked about the fact that a majority of the threats are related to insiders. This can be considered mistakes by employees as mentioned by Cheng et al. (2017). Contradictory, interviewee 2 explained how they categorize their risks into various categories, including internal and external risks. Since there is a high probability of something major happening, due to for instance internal or external threats.

5.2 Detection, prevention, and, announcement

The DLPD techniques are created to deal with data leakages and threats. By identifying and monitoring the threats, organizations can prevent data leakages (Cheng et al. 2017). When it comes to detecting a data breach, both interviewees highlighted the importance of acting on it quickly. By reporting it to the organization, and announcing it to everyone involved, including customers and employees. Like interviewee 1 and 2, Boban (2018) further added the importance of notifying a personal data breach to the supervisory authorities and to process the data systematically monitored. Both interviewees mentioned multiple times how the reporting to the authorities has become even more important and an obligation to avoid fines due to the new privacy laws of GDPR. Which is also brought up by Raman et al. (2011) and Boban (2018). This shows that GDPR has affected the way organizations work with detection, prevention, and the announcement today.

Brand image and reputation is something mentioned by both interviewees. They elaborated on the fact that a data leakage can have an impact on how the public views the organization. We can find that similarity, through the theoretical chapter. Caldwell (2012) and Ring (2013) mentioned that data leakage of any kind can cause harm to an organization's brand reputation and Raman et al. (2011) even explained that it could lead to decrease in an organization’s sales. An example can be the Sony incident when personal information from PlayStation Network got leaked and resulted in fines and cost of reputational damages (Ring, 2013).

Brockett and Golden (2012) and the interviewees see the value of monitoring and detecting cyber risks and threats. It is also important to note that spreading security awareness among employees supports the work of detecting and preventing. We found that this was also mentioned by Cheng et al. (2017), Mihaela (2019) and the interviewees. More specifically, interviewee 2 highlighted the importance of educating employees to spread awareness, as a part of the prevention process. Iguer et al. (2014) described that the primary source of risk is the organization’s employees. To support this statement interviewee 1 as mentioned above talked about insiders being a threat to the organization. Furthermore, this can be compared to the TTF model where the “ease of use and training” factor is used to describe and measure how well users, in this case employees, use the organization’s systems (Shahreki & Nakanishi, 2016; Liggett, 2020).

Our research shows that organizations working with detection and prevention want to make sure that information does not get exposed, intentionally or unintentionally (Cheng et al. 2017). More specifically, organization 2 works with prevention to help ensure that they work in a more systematic manner regarding information security. Together with monitoring and strengthening the detection prospects in relation to their Security Operations Center (SOC). In contrast,

interviewee 1 talks about prevention and reaction which is more about response and a bit about intelligence. The individual also mentioned that the detection process is about monitoring and follow-ups. We found a similarity when it comes to how both organizations view on detection because both interviewees highlighted monitoring as a part of the detection process. This resembles one of the purposes of DLPD, to detect by monitoring (Cheng et al. 2017).

5.3 The technological approaches

Interviewee 1 mentioned the use of the CIA triad when going through their security controls. The organization does also use log analysis for monitoring when trying to detect attacks. This goes in hand with the literature finding that analyzing and tracking logs is helpful when an organization wants to detect and prevent breaches (Cheng et al. 2017). As mentioned in the empirical findings, organization 2 finds it challenging to not cross over the lines when tracking logs to investigate a breach. The two interviewees could perhaps be talking about different types of logs. However, the conclusion can be drawn that log analysis could be a way of helping with detection. We believe it is a challenge for many organizations to try and find a good balance. As well as not going too far when scrutinizing, due to laws and avoidance of violations against privacy. Along with having enough information when investigating a data breach for instance. We think holding employees accountable for their actions and being able to trace back to a specific employee would help the organization with detecting and preventing leakage.

Interviewee 1 explains the need for: confidentiality, integrity and availability, as a part of the technological approaches. Similarly, the article by Mihaela (2019) discusses the need for confidentiality, integrity, and availability of data storage and processing in any security system. Even Iguer et al. (2014) elaborated on the importance of the usage of the CIA triad. Similarly to that, interviewee 2 highlight the vulnerabilities of systems as their SOC is there to monitor identified errors.

The Multi-agents system (MAS) is mentioned in the article by Iguer et al. (2014) and it is explained that the systems architecture needs to fulfill certain requirements, including: extensibility, reactivity, programmability, etc. Both interviewees talked about some important aspects regarding the requirements that need to be fulfilled to make out a useful application or system. However, they do not specify the types of requirements used to implement a system or application. Which does not give a detailed description of the criteria a system within the organizations has.

The system's quality of newly implemented systems is a part of the technological approach and affects the digital environment of the organizations. In regard to the TTF model the factor about system reliability is about depending and relying on the systems (Shahreki & Nakanishi, 2016;

Liggett, 2020). We also think that this factor of the TTF model can support the technical approach within organizations.

According to interviewee 2, there is a need for analysis of the systems requirements. So, when developing systems with sensitive information, it is necessary to have a stronger security. That can include passwords and fingerprints. By doing that it keeps the system's quality high and risk-based. We think that this is a useful way of ensuring a system's quality since it shows that there is a thoughtful process followed to obtain quality. On the other hand, interviewee 1 highlighted their complex mass requirements that are important when implementing a new application. There is a classification process followed that filtrates the requirements so that the most relevant requirements are used. It can be considered a part of the system's quality check. We also think that this strategy is thoughtful but we believe that it is more complex because it requires more focus on the details and the specific requirements of a system or application.

As presented in the survey, most individuals choose the in-house data handling method as the safest, but this result can be difficult to interpret since these respondents are individuals who may not have as much knowledge about the subject as someone who works with it. Both interviewees say that they have outsourced data to third and fourth parties. They also highlighted that it is important to ensure their outsourced partners handle the data the right way with high security. Since data can also be leaked through third and fourth parties (Raman et al. 2011).

Lastly, interviewee 2 made an interesting point where the individual talked about the importance of a need for a system, before implementing it. Since all technological implementations are important, it may not solve all problems that are security related. Using Oscarsson (2019) argumentation, he similarly explained that security went from being a technical concern for mainly the IT-department to becoming a concern on business level. This means that security is more than technology. Nonetheless, interviewee 1 does not highlight any such aspects or point about the technological implementations.

5.4 Authorization of data and awareness

The authorization is another key factor in the TTF model and is explained by both interviewees as being one important aspect. Both interviewees talk about the need for acceptance by customers when authorizing their data, better communication, and making it easier for the customer to understand their rights and how their data is being used. This has in return led to more assessments and awareness together with an understanding from the business. A part of the awareness aspect is the reporting of any concern regarding data leakage. We found in the survey results that almost 30% think organizations do not give enough information about their data handling. Whereas 54% of the respondents think organizations sometimes give them enough information, regarding the handling of their data. At the same time the survey showed that individuals are aware of security. Which in this case, shows that organizations are perhaps not

doing enough to inform their customers or the information provided is not very clear. An important point related to this, highlighted by interviewee 2, is to not have long "informational essays" when informing customers. We believe a better way could perhaps be to make a bulleted list of the most necessary information. The full text with the information could then be accessible with the list through a link or somewhere else easily accessible for the reader. This is something that Ooijen and Vrabec (2019) and Corradini (2020) also argued about. Since the respondents were not answering about these specific organizations that were interviewed. It is hard to say how well both organizations have accomplished their cybersecurity goals, from an individual's point of view. In general, this could be an area organizations can improve because it would be easier for the reader to understand, increase awareness and show that organizations are actively working towards protecting individuals' data.

The survey results also showed that the awareness of data breach issues in individuals is high, with almost 75% of them answering *Yes* on if they are aware of it. Almost half of them think about the handling of their data by organizations and the level of concern is on a three (3) on a scale from 1 to 5. They are also mostly concerned about stolen credit card information, which is information many organizations handle or come in contact with. This showed that individuals are quite aware of how their data is handled by organizations. This is also confirmed in the literature by Corradini (2020) but she also argued that individuals may not be aware of the whole process of the handling of their data (Corradini, 2020).

GDPR gives EU citizens the rights over their own data. The new rules are strengthening already-existing rights due to the increasing concern amongst European citizens, regarding the use of their personal data by organizations (Boban, 2018). Besides informing customers about their rights and reporting a data breach to the organization and everyone involved. Interviewee 1 and Interviewee 2 both mentioned the obligation to report to the authorities. Both interviewees highlighted that GDPR has given positive effects on the security work of the organizations. Employees have become more aware and are more careful when handling sensitive data and information. The fear of doing something wrong has become more common. The findings can show that the effects of GDPR can cause the internal, unintentional threats to decrease. Since an employee is more likely to give a second thought of what a document or e-mail contains before publishing or sending it. Both interviewees comment on the positive effects and changes GDPR has caused. Interviewee 1 even says it has given them opportunities to do changes and adjustments on products and applications they would not have done otherwise.

5.5 Prospects

Regulations for carrying out law enforcement to international criminals can be a challenge even close to impossible (Brockett & Golden, 2012). Our interviewees discussed the challenges of different interpretations of laws and regulations. One concern could be that cross-border legislation follows rules that may differ from the host country, described by interviewee 1 and 2.

Interviewee 1 emphasized on the fact that the storage of data poses a challenge. It can be difficult to know where customers' data is allowed to be stored, depending on where the customer lives. For instance, will it be allowed to store data from customers in Russia in another country? Interviewee 1 explained that they have employees working with these questions and it is a part of the prospects.

The TTF model can be used by organizations to understand the relation between an aspect in security and their business continuity plans. Key factors such as "quality" and "authorization", or other security purposes and business continuity plans, can be used in this model. For instance, by putting "quality" or a security process into the Technology Characteristics box of the model and putting business continuity into the Task Characteristics box. The relationship between these two boxes can then be evaluated and the organization gets the effects, which would be the fit (See figure below). By doing something similar, organizations can get an idea of how some of their key factors and ways of handling things regarding security are concerning their business continuity plans. If they are a fit and affect each other positively or if something needs improvement. As mentioned by interviewee 1, a part of their strategy is the business continuity planning. This helps the organization (1) to ensure that their business works, and that the teams can quickly continue with their work even if a disruption or a sudden event were to happen.

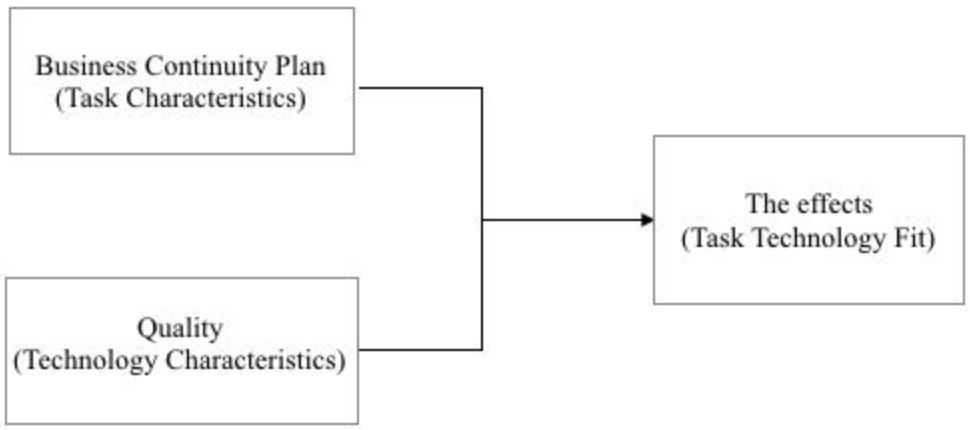


Figure 5: Our own application of a part of the TTF model.

6 Conclusion

This chapter summarizes this research study by answering the research question. The first section describes how the study has answered the research question and the results presented. The last section provides an understanding and suggestions for future research within this area.

To answer our research question: *What are the organizational security measures and the individual perception of an organization's security attempts?* A set of challenges and security measures are presented in the discussion. The interviewees have contributed with key knowledge regarding the measures taken to combat cybercrime. The survey results present how much knowledge and concern individuals have regarding the subject of cybercrime.

Similarities and some differences could be found between organization 1 and 2, regarding their security measures, handling of customer data and future challenges.

Our study shows that organizational security measures are complex and is a challenge they continuously work with. From the empirical findings it is evident that these challenges within the security spectrum are not restricted to the IT-departments because it impacts the organization as a whole. Moreover, it is indicated that security is influenced by legal requirements, more specifically the laws and regulations of GDPR.

Furthermore, we found that a majority of the survey participants believe that they do not get provided with enough information, regarding the utilization and handling of their data. The results, together with the literature, highlight the differences between individual knowledge and awareness.

An important conclusion is that organizations mention the importance of communication with customers and providing them with comprehensible information about their data handling. However, our survey results indicate that individuals' perception of their data handling by organizations differs. Organizations can take these results into consideration and improve their communication.

As mentioned previously, problematizing these challenges is not the intention of this study. Therefore, the results found in our research can be utilized as a guide for organizations or future research.

6.1 Future research

The world of technology and more specifically IT can be relatively complex and rapidly developing. In the future the scope of this research could be narrowed down and the focus be to investigate customer relationship management (CRM) or how companies educate their staff and raise awareness within the field of security. The research can further be developed by investigating more companies and more individuals. To get a broader perspective on the relationship between an organization and its customers.

7 References

Accenture. (2019). The cost of cybercrime - Ninth annual cost of cybercrime study, [pdf], Accenture and Ponemon Institute LLC. Available online: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf [Accessed 2020-03-20].

Alqahtani, H. & Kavakli-Thorne, M. (2019). Does Decision-Making Style Predict Individuals' Cybersecurity Avoidance Behaviour?, in Moallem, A (ed), *HCI for Cybersecurity, Privacy and Trust*, Springer, Cham, pp. 32-50.

Bishop, L. M., Morgan, P. L., Asquith, P. M., Raywood-Burke, G., Wedgbury, A. & Jones, K. (2019). Examining Human Individual Differences in Cyber Security and Possible Implications for Human-Machine Interface Design., in Moallem, A (ed), *HCI for Cybersecurity, Privacy and Trust*, Springer, Cham, pp. 51-66.

Boban, M. (2018). Cyber Security Foundations For Compliance Within GDPR For Business Information Systems, *35th International Scientific Conference on Economic and Social Development –"Sustainability from an Economic and Social Perspective",* pp. 541-553.

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A. & Maimon, D. (2019). Designing and Evaluating Crime Prevention Solutions for the Digital Age. *Cybercrime Prevention*, pp. 125-146.

Brinkmann, S. (2013). Qualitative Interviewing (Understanding Qualitative Research). Oxford University Press Inc., [e-book], Available through: LUSEM Library website http://www.lusem.lu.se/library, pp.144-145, [Accessed 2020-05-10].

Brockett, P., & Golden, L. (2012). Enterprise Cyber Risk Management. *Risk Management for the Future - Theory and Cases,* Chapter 14, pp. 319-340.

Buckman, J., Hashim, M. J., Woutersen, T. & Bockstedt, J. (2019). Fool Me Twice? Data Breach Reductions Through Stricter Sanctions. *SSRN*.

Caldwell, T. (2012). Reporting data breaches. *Computer Fraud & Security*, vol. 2012, issue 7, pp. 5-10.

Cheng, L., Liu, F. & Danfeng, Y. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *WIREs Data Mining Knowl Discov 2017*, vol. 7.

Corradini, I. (2020). Building a Cybersecurity Culture in Organizations - How to Bridge the Gap Between People and Digital Technology. [e-book] Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 2020-06-20].

Creswell, J. W. & Clark, V. L. (2011). Designing and conducting - Mixed Methods Research. SAGE Publications Inc., California.

Culp, S. (2019). Cybercrime: A Major Threat To Trust In The Digital Economy, Available online: https://www.forbes.com/sites/steveculp/2019/03/25/cybercrime-a-major-threat-to-trust-in-the-digital-economy/#ef24cd62cb77 [Accessed 2020-05-18].

Cusick, J. (2018). The General Data Protection Regulation (GDPR): What Organizations Need to Know. Available online: https://www.researchgate.net/publication/323538588_The_General_Data_Protection_Regulation_GDPR_What_Organizations_Need_to_Know [Accessed 2020-06-15].

Das, S. & Nayak, T. (2013). Impact of Cyber Crime: Issues and Challenges, *International Journal of Engineering Sciences & Emerging Technologies*, vol. 6, issue 2, pp. 142-153.

Frydlinger, D. Edvardsson, T. Carlström, C. O. & Beyer, S. (2018). GDPR: - juridik, organisation och säkerhet enligt dataskyddsförordningen, Norstedts Juridik AB, Stockholm.

Furnell, S., Khern-am-nuai, W., Esmael, R., Yang, W. & Li, N. (2018). Enhancing security behaviour by supporting the user. *Computers & Security*, vol. 75, pp.1-9.

GDPR.EU. (2020). What is considered personal data under the EU GDPR?, Available online: https://gdpr.eu/eu-gdpr-personal-data/ [Accessed 2020-05-05].

Ghernaouti, S. (2013). Cyber Power - Crime, Conflict and Security in Cyberspace. EPFL Press, Lausanne, Switzerland, p.5

Goodhue, D. L & Thompson, R. L. (1995). Task-Technology Fit and Individual Performance. *MIS Quarterly*, vol. 19, no. 2, pp. 220, 225.

Gravetter, F. J. & Forzano, L. B. (2009). Research Methods for the Behavioral Sciences. Wadsworth Publishing, California.

Hartelt, R., Wohlfeil, F. & Terzidis, O. (2015). Process Model for Technology-Push utilizing the Task-Technology-Fit Approach. *19th Interdisciplinary Entrepreneurship Conference*.

Heickerö, R. (2012). Internets mörka sidor. Om cyberhot och informationskrigföring. Bokförlaget Atlantis, Stockholm.

Information Commissioner's office. (2020). Security, Available online: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ [Accessed 2020-05-15].

Iguer, H., Medromi, H., Sayouti, A., Elhasnaoui, S., Faris, S. (2014). The Impact of Cyber Security issues on Businesses and Governments: A framework for implementing a Cyber Security Plan, *2014 International Conference on Future Internet of Things and Cloud*.

Jacobsen, D. I. (2002). Vad, hur och varför - om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen. Studentlitteratur, Lund.

Leukfeldt, R. (2017). Research Agenda - The Human Factor in Cybercrime and Cybersecurity. Eleven International Publishing, The Hague.

Liggett, R. (2020). The Effects of Information Security on Business Continuity: Case Study. ProQuest LLC, Michigan.

Mihaela, C. L. (2019). Current security threats in the national and international context. *Accounting and Management Information Systems*, vol. 19, no. 1, pp. 351-378.

Moore, S. & Keen, E. (2018). Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. Available online:

https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019 [Accessed 2020-05-15].

Oates, B. J. (2006). Researching Information System and Computing, SAGE Publications Ltd, London.

Ooijen, I. V. & Vrabec, H. U. (2019). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy,* pp. 91-107.

Oscarsson, P. (2019). Informationssäkerhet, Studentlitteratur AB, Lund.

Patel, R. & Davidson, B. (2011). Forskningsmetodikens grunder - Att planera, genomföra och rapportera en undersökning. Studentlitteratur AB, Lund.

Purcell, A. (2018). 3 key ideas to help drive compliance in the cloud. IBM. Available online: https://www.ibm.com/blogs/cloud-computing/2018/01/16/drive-compliance-cloud/ [Accessed 2020-06-15].

Raman, P., Kayacık, H. G. & Somayaji, A. (2011). Understanding Data Leak Prevention. *6th Annual Symposium on Information Assurance, Academic track of the 14th Annual 2011 NYS Cyber Security Conference,* pp. 27-31.

Ring, T. (2013). A breach too far? *Computer Fraud & Security*, vol. 2013, issue 6, pp. 5-9.

Sapsford, R. (2007). Survey Research. [e-book], Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 2020-05-05].

Shahreki, J. & Nakanishi, H. (2016). The Relationship between Task Technology Fit and Individual Performance: Case Study in Hotel Industry in Malaysia. *Journal of Soft Computing and Decision Support Systems* (*JSCDSS)*, vol. 3, no. 6, pp. 1-15.

Stallings, W. & Brown, L. (2018). Computer Security: Principles and Practice. Pearson.

Thompson, N., McGill, T. J. & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, vol. 70, pp. 376-391.

Verizon. (2020). 2020 Data Breach Investigations Report, [pdf], Available online: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf [Accessed 2020-05-19].

8 Appendices

Appendix 1 - The Interview Guide

Ethical aspect

CONTRACT
1. Permission to record the interview and thereafter transcribe the conversation
2. Asking if the interviewee wants to stay anonymous or if he/she will allow his/her name and title to be mentioned in the research?
3. Inform the interviewee that: the material gathered from the interview will solely be used for the research purpose and the publication of a BSc thesis
4. The interviewee can choose to cancel the interview at any time
5. Are the statements mentioned above accepted by the interviewee?
6. The interviewee will be informed that the completed research thesis will be sent to him/her if he/she wishes so
7. First and foremost, the purpose of the research presented: a. Presentation of the authors and the thesis b. Presentation of the research topic

Introductory questions about the interviewee

QUESTION(S)
1. Tell us a little about you. What is your role within the organization?
2. How long have you been working with this specific role?

3. What background do you come from before you joined the organization?
4. What are your main responsibilities within the organization?
5. Something that signifies your organization and department? a. How would you explain and define your organization's and department's working environment?
6. How can a typical workday look like for you?

Cyber Security, Cyber Crime and Threats: Risk Management Perspective

QUESTION(S)
1. What does Cyber Crime entail for you? What does Cyber Security entail for you?
2. Does your organization separate the risk types into categories? a. Such as Internal and External risks, and if so, how are these managed? b. What are the financial effects of Cyber-threats and the risks that follow?
3. Does your organization have a Risk Management Process tailored to: a. Mitigate and control Cyber-threats?

Data Breaching

QUESTION(S)
1. What do you know about the term Data Breaching?
2. How would a Data Breach affect your organization? a. Financially? - b. Reputation and Brand image? From a customer's perspective and an employee's perspective?
3. Technology is constantly changing, what does your organization do to keep your System's Quality high together with keeping employees and customers up to date?
4. How does the GDPR affect the way your organization works with detection, prevention and announcing a Data Breach?

Implementation of a Plan and Strategies Concerning Cyber Security and Cyber Crime: Data Breach Perspective

QUESTION(S)
1. Could you explain what plan or strategy(s) your organization has developed to combat Cyber Crime and prevent Cyber-attacks such as: a. Data Breaches?
2. Has your organization had any Data Breach, external or internal (as a direct effect from your mitigation plan or strategy)?
3. From a technological and a software point of view, can you elaborate on the technical reliability within the organization?

Challenges concerning Cyber Crime regarding Information and Cyber Security: Data Breach and its challenges

QUESTION(S)
1. How does your organization tackle threats and challenges, such as: a. Data Breaches?
2. Are there any issue(s) that cannot be solved before a Data Breach has occurred? a. What proactive measures are taken?

GDPR

QUESTION(S)
1. How does your organization work with GDPR? a. How does your organization manage the personal data and information of your *employees*? b. How does your organization manage the personal data and information of your *customers*?

2. How does your organization work to ensure that your customers are aware of the organization authorizing their data?

Implementation of a Plan and Strategies concerning GDPR

QUESTION(S)
1. What were the key factors your organization focused on when getting ready for the GDPR implementation?
2. Since the introduction of GDPR in 2018, what has changed in the way your organization handles data and information from: a. Employees b. Customers

Challenges concerning GDPR

QUESTION(S)
1. Is there any current challenge(s) that your organization has to deal with concerning GDPR? a. Concerning the implementation of the new GDPR laws?
2. Any previous challenge(s)? Possible future challenge(s)?

Conclusion

QUESTION(S)
1. Do you have any other comments or feedback that you want to contribute with?

Appendix 2 - The Survey Guide

The Survey
Definitions: **Data breaching:** A data breach is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner. **Cyberattack:** An illegal attempt to harm someone's computer system or the information on it, using the internet. **Outsourced data:** When an organization hires an outside organization to perform services or tasks such as handling their data. **In-house data:** When data is handled within an organization.
1. **Gender:** Male Female Other:
2. **Age:** 16-25 26-49 50-65 Over 65
3. **Occupation:** Student Employed Unemployed Other (Eg. Student and Employed)
4. **Are you aware of data breaching*(leakage) issues within organizations?** Yes, No, Not sure

5. If yes, which of the following data breaching*(leakage) issues concerns you the most: (rank them in order of most concern) Stolen identity information Stolen credentials (username/password) Stolen credit card details
6. Have you ever thought about how your data is being handled by organizations? Yes, No, Sometimes, Not sure
7. If yes, which data handling procedure would make you feel the safest: Outsourced data* to a third party with a known reputation In-house data* handling with the latest technology
8. To what extent are you concerned that your data can be leaked due to for instance cyber attack(s)* or technological errors within organizations? 1-5 (scale)
9. GDPR is often referred to as the strongest regulation ever created. Do you know what capability GDPR has to protect you? Yes, No, Not sure
10. Do you think that organizations handling your data gives you enough information about how they authorize your data Yes, No, Sometimes, Not sure

Appendix 3 - Transcription Interview 1 [Int 1]

Interviewee: Interviewee 1 (Anonymous)

Interviewers: Sarah Shahid and Emelie Huang

Date of interview: April 6th, 2020 (Part 1) & April 14th, 2020 (Part 2)

Location of interview: Online platform (Microsoft Teams)

Line	Person	Questions and answers
		PART 1
1.	Interviewer	Permission to record the interview and thereafter transcribe the conversation.
2.	Interviewee 1	Ja, men precis, precis, och jag tror att det finns till och med automatisk transcription. Vet inte om det fungerar på svenska dock.
3.	Interviewer	Men vi fick i alla fall göra det?
4.	Interviewee 1	Ja, absolut.
5.	Interviewer	Asking if the interviewee wants to stay anonymous or if he/she will allow his/her name and title to be mentioned in the research? Och ni vill vara anonymous?
6.	Interviewee 1	Ja, asså jag vill gärna att namnet på företaget ska vara anonymt. Men om ni ger mitt namn så kan de trace:a tillbaka, så vem som helst kan trace:a tillbaka till företaget. Så det är lika bra att både mitt namn och mitt företags namn, i det ni publicerar, och sen när ni diskuterar med handledare och internt inom universitet och sånt, det, (paus) Så länge det inte finns skriftliga spår.
7.	Interviewer	Inform the interviewee that: the material gathered from the interview will solely be used for the research purpose and the publication of a BSc thesis. Detta används bara för vår thesis.
8.	Interviewee 1	Jag förstår. Jo, det är ok.

9.	Interviewer	The interviewee can choose to cancel the interview at any time. Så du har rätten till att cancel när du vill.
10.	Interviewee 1	Ja, ja men vi kör tycker jag. Asså det, jag förstår. Tack att jag får möjlighet att få göra det. Det är lugnt.
11.	Interviewer	Are the statements mentioned above accepted by the interviewee? Och det är dem?
12.	Interviewee 1	Ja.
13.	Interviewer	The interviewee will be informed that the completed research thesis will be sent to him/her if he/she wishes so
14.	Interviewee 1	Absolutely. Jättegärna. Det (paus) finns det möjlighet och läsa ert arbete så gör jag det gärna.
15.	Interviewer	Ja, perfekt. Och sen skulle vi bara göra en liten presentation om vår research och topic.
16.	Interviewee 1	Ok, absolut.
17.	Interviewer	Ok, vår frågeställning är “What are the critical security measures in information security?”. Så basically typ vilka säkerhetsåtgärder ni tar när det kommer till säkerhet i företaget. Och vi är som sagt två studenter från Lunds universitet. Vi läser sista året just nu, sista terminen, Systemvetenskap. Vi är väldigt intresserade av information security.
18.	Interviewee 1	Ja, vad roligt ja.
19.	Interviewer	Ja.
20.	Interviewee 1	Kul. Vad bra. Ja men vi kan gå igenom era frågor om ni vill. Om ni vill ha det så strikt, annars kan jag bara babbla på. Asså jag utvecklar gärna lite för att, ni ställer frågor som är relevanta. Jag tycker man skulle kunna bädda ut detta genom att prata om governance och ni pratar lite grann om det, jag har en fråga kring strategin, vilket jag tycker är grunden, inte strategi i sig, men governance i alla fall, grunden till strukturen.

21.	Interviewee 1	Hur informationssäkerhetsarbete organiseras och delegeras i företaget och har man inte det på plats så spelar det ingen roll att man har risk management process till exempel för att det är ingen som tar ansvar för risker. Det är ingen som tar ansvar för att göra risk assessments och det är ingen som tar ansvar för mitigation och controls och action plans och så vidare...
22.	Interviewee 1	Så jag kommer dra tillbaka till governance hur ofta jag kan. Jag hoppas att det också ger en helhetsbild då, som i syfte knyter ihop dem frågorna som ni ställer. För det är väldigt brett, så det finns väldigt mycket att berätta. Jag tyckte att det var rätt valda områden men jag vill gärna kunna hålla mig till, eller knyta tillbaka till governance modellen då.
23.	Interviewer	Yep, ok första frågan då. Det är mer liksom, tell us a little about you. What is your role within the organization?
24.	Interviewee 1	Lite om mig.
25.	Interviewer	Mm.
26.	Interviewee 1	Så jag har jobbat på (organisation 1) som anställd i tre år och innan dess har jag faktiskt konsultat ett par år, i olika projekt inom payments, security, compliance (paus) security compliance (paus) så nu jobbar jag inom informationssäkerhetsteamet som heter Group Information Security and Data Privacy. Vårt mål är både att ta hand om det strategiska vad gäller båda infoSec och data privacy. Knyta till GDPR vad gäller data privacy såklart men också vad gäller de tekniska åtgärder för att implementera data privacy och GDPR. Innan dess så har jag jobbat på big four bolagen som är stora konsulting revisionsbyråer, KPMG och PwC inom cybersecurity och informationssäkerhet.
27.	Interviewee 1	Cyber är en ganska ny terminologi, en ny term som inte användes så mycket tidigare. Det är ett begrepp som försöker inkludera allt men man menar oftast olika saker, eller olika personer menar olika saker så vi kan komma till det sen... för att jag tror det var en fråga om cybersecurity eller cybercrime och vad det är för något och det är viktigt att sätta en definition och vara överens, så vet vi vad vi pratar om.
28.	Interviewee 1	Min roll är reporting manager, en lite mer komplicerad titel än så men det handlar om att kunna visualisera hur vi ligger till vad gäller informationssäkerhet och data privacy. Rapportera till organisationen, då till management board om vår current state of security, current state

		of privacy, om våra risker och eventuella positiva trender också. I slutändan handlar det om att lyfta upp top 5 risks vad gäller säkerhet och privacy.
29.	Interviewee 1	Den rollen har jag haft sen efter sommaren förra året och det var rätt i kontinuitet med det jobbet som jag gjorde redan innan, som information security leader. Det vill säga om att säkerställa att vi har en internal control framework, ett subsätt of control som vi säkerställer appliceras till alla applikationer, produkter, digitala produkter. Våra regler definieras i form av en control oftast, men också en ansvarig för att implementera den kontrollen för en tidsaspekt och när det förväntas att den kontrollen ska implementeras eller hur ofta den ska granskas till exempel. Hur ska jag implementera och så vidare och det är det man kallar för "5 W": who, when, what, how, where.
30.	Interviewer	Ja.
31.	Interviewee 1	Jag hoppar över till, jag försöker ändå följa strukturen som ni har föreslagit.
32.	Interviewer	Mm.
33.	Interviewee 1	Ja, background, innan jag började på (organisation 1) har ni fått höra. Så jag har mer än 20 års erfarenhet inom informationssäkerhet och cybersecurity. Jag vet inte om det ger nån form credit men i alla fall att man har varit med i en viss utveckling. Jobbat från början med många cyber, IT säkerhetsfrågor relaterade till infrastruktur och applikationer för att jobba, fortsätta som security arkitekt och jobba mer med taktiska frågor och projekt för att de 10 senaste åren jobba mer strategiskt. Antingen som konsult eller numera på (organisation 1).
34.	Interviewee 1	Juste, om jag kan beskriva organisationen. Hur vi struktureras inom säkerhet och privacy och även inom risk inom bolaget är att vi är ett strategiskt team som på sikt, vi har ett team på 21 personer, vi är inte där än men vi är ungefär 20 personer kan man säga. Med lite olika ansvarsområden inom data privacy till exempel. Det finns personer som jobbar med focus som EU-länder och andra länder som vi jobbar i såklart.
35.	Interviewee 1	Utanför EU, har vi lite olika businesses också. (organization 1), som ni vet, består av som vi kallar för (sekretess) Vi har en stor del av vår försäljning som sker online också och sen har vi lite annan butik.

		(sekretess)
36.	Interviewee 1	Då har vi inom mitt team personer som är som point of contact mot antingen investments, centers och mot som sagt EU länder, icke EU-länder. Vi har också ett cyber team som, nu har jag inte den exakta siffran men det närmar sig kanske 50 pers som jobbar inom olika områden och som både stöttar business och utvecklingsteamen. Däremot är de också organiserade i ett team för protect för att skydda infrastruktur och applikationer. Detect med allt som handlar om monitorering och uppföljning. Prevents och react som handlar om response, lite grann om intelligence också, eller bug bounty.
37.	Interviewee 1	Sen finns det ett team som gör data privacy granskningar, assessment och en annan som gör informationssäkerhet assessments. Det handlar om att följa upp om vår cyberförsäkring till exempel, eller internal audits, financial audits. Det finns olika externa granskningar mot oss som vi stödjer inifrån och som vi måste förbereda såklart. Så det finns teams som tar hand om sånt. Så ni har lite grann om den strukturen.
38.	Interviewer	Mm.
39.	Interviewee 1	Var är vi nånstans nu?
40.	Interviewer	Nummer 4.
41.	Interviewee 1	Vad sa du?
42.	Interviewer	Fråga nummer 4 men du har typ svarat på den frågan, your main responsibilities within the organization?
43.	Interviewee 1	Ja, ja precis. Som sagt så är jag Reporting Manager.
44.	Interviewer	Exakt.
45.	Interviewee 1	Så säkerställa just att vi följer upp om implementation av våra demands och requirements men också lyfter upp eventuella gaps och mäter mognadsnivå för att kunna lyfta, rapportera våra risker och våra trender.
46.	Interviewer	Exakt, du har precis svarat på den här, something that signifies your organization and department?
47.	Interviewee 1	Ja, exakt.
48.	Interviewer	Du har berättat om hela strukturen. Så vi behöver inte ta det igen.

49.	Interviewee 1	Ja.
50.	Interviewer	How can a typical workday look like for you?
51.	Interviewee 1	Så, jag har 3 huvuduppgifter. Den ena är att såklart bygga upp den där reporting capability. Så det tar ganska mycket av min tid och samordnas med resten av organisationen för att det, jag behöver input från andra, jag behöver komma överens med vissa personer också om hur vi ska göra det på det bästa sättet.
52.	Interviewee 1	En annan aspekt av mitt arbete är att hjälpa i projekt, så vissa stora projekt som drivs under flera års tid kan de behöva stöd från strategiska perspektivet och då kan jag hoppa in och hjälpa till och vara deras single point of contact. En annan aspekt och den tredje då är att säkerställa just implementation av de processer och kapabiliteter som vi sätter upp.
53.	Interviewee 1	Så för att till exempel ska kunna mäta om efterlevnad, behöver vi ha nån form av compliance process på plats. Så etablering av antingen en compliance process vad gäller InfoSec och data privacy kan vara mitt ansvar. Implementation av detta, dvs. hjälpa businessen med att säkerställa det som har gjorts, kan vara en annan aspekt som är lika viktigt och det hjälper med väldigt mycket att förstå vad det är som brister i de processer som jag kan vara med och etablera. Så, för att bättre kunna optimera det framöver och så vidare så jag är med i delvis implementation av de processer som jag oftast bidrar att sätta upp.
54.	Interviewee 1	Så cyber (paus) and threats: risk management. Så vad betyder cybercrime för mig och cybersecurity. Så för mig handlar cybersecurity om den tekniska implementationen av informationssäkerhet. Så det handlar om operational security, eller IT säkerhet. Det vill säga att teamen som tar hand om att säkra vår infrastruktur, monitorerar för attacker, åtgärdsarbete. Så, det är lite grann det som omfattar cybersecurity, så det är inte hela säkerhetsarbetet, det är det operationella.
55.	Interviewee 1	Enligt tidigare erfarenheter så brukar man kalla cybersecurity, asså det är ett trendigt ord så man kallar allt för cybersecurity till exempel som inom PwC där det fanns en ganska stor, cybersecurity avdelning som också tog hand om strategiska frågor men också väldigt mycket om operationella frågor. Så, det var ett stort team som bidrog med konsulter för att hjälpa företag med specifika uppdrag. Så det kunde vara både

		högt och lågt och strategiskt och operationellt, och så vidare… Så jag har förståelse eftersom jag också har jobbat som konsult inom väldigt många olika bolag, inom olika branscher.
56.	Interviewee 1	Man menar olika saker med cybersecurity men inom mitt bolag idag (organisation 1), definierar cybersecurity den operationella delen. Jag är överens om den beskrivningen. Vad gäller cybercrime, det handlar om både frauds och attacker, både interna, externa attacker, insider attacker och ja, det kan vara organiserad kriminalitet. Så, cybercrime, jag är lite nyfiken och höra hur ni definierar cybercrime och cybersecurity så att vi kan komma överens om den definitionen.
57.	Interviewer	Ja, ganska lik din definition. Vi har kanske lite mer generell definition, du fokuserar mer på själva företaget också. Cybersecurity är typ all data som kanske rör företag eller governments. Cybercrime är liksom ja, hackers som gör attacker, eller cybercriminals som tar känslig data från företag eller governments.
58.	Interviewee 1	Inte insiders?
59.	Interviewer	Vad sa du?
60.	Interviewee 1	Insiders attacker, räknas det inte som cybercrime?
61.	Interviewer	Jo, det gör det.
62.	Interviewee 1	Det är det också, ja. Mer än hälften av alla attacker som sker är på grund av interna personer.
63.	Interviewer	Ja, exakt. Vi läste någon artikel att det var internal attacks.
64.	Interviewee 1	Det beror på vad man mäter också.
65.	Interviewer	Ja.
66.	Interviewee 1	Roligt att ni ställer just den frågan. Jag tycker att den är väldigt relevant vad gäller risk, risk universe som det heter. Vi håller på att revidera vår risk management process och flika in, uppdatera vår risk universe också. Oavsett vad vi är i den utvecklingen så har vi faktiskt risker delade i olika kategorier. Ja, både inom strategiska risker, business operations, social, och hållbarhet, också att vi lägger vår compliance, legal och compliance som en riskkategori i sig, finance och technology. Informationssäkerhet och cyber finns delvis inom technology, men jag

		skulle säga inom alla områden. Så det finns inte kategorier i sig eftersom den finns överallt. Cyber specifika risker är mest riktade till teknologin så det finns under det område och (paus). Behöver ni tid eller?
67.	Interviewer	Ja, en sekund bara.
68.	Interviewee 1	Yes. Är det högljutt i biblioteket?
69.	Interviewer	Ja, det är lite högt bakom. Fast vi hör dig nu, mycket bättre.
70.	Interviewee 1	Alright, ok. Vad bra. Så vart var vi nånstans? Riskkategorier. Internal, external risks, inte så mycket definierat på det sättet, nej. Men som sagt inom risk universe så tror jag inte vi har uppfunnit hjulet där asså vi baserar förmodligen vår risk universe på kända och väl adapterade ramverk.
71.	Interviewee 1	(läser upp frågan) Financial aspects, ja, financial är en av kategorierna i vår risk universe. What is the financial effects of cyber-threats and the risks that follow? Vill ni förtydliga den frågan?
72.	Interviewer	Ja, vi tänkte mer på liksom när ni får nån cyber threat, vad är det, vilka financial effects har det på er liksom organisation. Asså dessa threats och crime, hur påverkar det er liksom, the financial aspekt av er organisation.
73.	Interviewee 1	Ja, det är en väldig svår fråga att besvara. Asså låt säga, information, säkerhet och cyber har kanske nån form av top management. Det (paus) en av dem prioriteter som finns och hantera med ledningsaspekt. Så det finns en stor impact om vår business skulle råka på en läckage eller böter från myndigheter. Det (paus) asså om det skulle vara en läckage av (paus), en väsentlig läckage, personuppgifter, persondata så skulle straffet kunna vara ganska högt i relation med vår turnover internationellt...
74.	Interviewee 1	O det är ingenting som vi önskar exponerar oss mot såklart. Så det finns verkligen en stor attention för att vara ehh proaktiva o inte riskera en sån läckage. Sen vad gäller risk så jag skulle säga risk är alltid en tolkning av ehh man har alltid en aptit för risk och olika toleransnivåer, på olika..., inom olika områden ehm och då är det väldigt kostsamt att skydda sig mot de absoluta risker. Låt säga “nej, vi (paus) och det går inte heller”. Så företag måste alltid ta beslut om, ok, till vilken nivå behöver vi skydda detta?

75.	Interviewee 1	Kan ta ett exempel, så, visst är det dramatiskt om personuppgifter skulle läcka ut. Jag pratar inte specifikt relaterad till (organisation 1) nu, jag pratar allmänt. Och, ja, så vad skulle det kosta att skydda ehh en specifik applikation så att information inte kan läcka. Så man tar alla möjliga åtgärder.
76.	Interviewee 1	Först skulle det vara väldigt svårt att jobba inom den applikationen, vara restriktiv, det finns skäl till nån form av kompromiss mellan operationella behov, funktionella behov, icke-funktionella behov och sen säkerhet. Så det är en tid man försöker backa in säkerhet så mycket som möjligt men ibland så kräver den funktionaliteten att man accepterar att en viss åtgärd inte finns på plats. Och skulle man lägga fokus på att skydda att en (1) personuppgift skulle läcka ut, skulle det kosta enormt mycket...
77.	Interviewee 1	Om har man däremot en limit som är, ok låt säga över 2000 personuppgifter, börjar bli väldigt kritiskt för företaget, om det läcker mer än 2000 personuppgifter eller 200. Jag behöver inte sätta en limit så här och säga det är 2000 som gäller. Så man kan sätta åtgärder så att från och med 200 personuppgifter som antingen processas på en gång eller transporteras på en gång. Då ska vi sätta ytterligare åtgärder så att de inte kan läcka. Men det är inte när man bara överför en personuppgift. Det är när man överför 200 eller mer än 200.
78.	Interviewee 1	O man kan säkert (bryts) på dem..., på den applikationen o hur den fungerar genom att, “ok ni får inte skicka bara en personuppgift för att det är för kostsamt för oss att skydda när ni bara skickar iväg en personuppgift”. Det skyddet, det är alldeles för kostsamt. Så ni får vänta tills ni har samlat 200 innan ni skickar dem iväg och då har ni de åtgärderna på plats. Så, jag vet inte om jag förklarade det så pragmatiskt men det jag vill säga är att varje business unit på nåt sätt får sätta sin tolerans och säga “ja, den typ av risk kan vi leva med”, “den typ av risk kan vi inte leva med”.
79.	Interviewee 1	Oftast handlar det inte om att tolka lagen. Det handlar om att, ja, “vad skulle risken vara att vi mellan en business unit till en annan business unit inte krypterar data just nu”. “Ja, för att ni skickar så lite data åt gången så är det kanske inte så farligt. Skulle ni skicka stora mängder av data så skulle vi kunna exponera oss på ett annat sätt, isåfall får ni hitta andra åtgärder.” Ja, så, apropå risk, det vill säga, det handlar inte så mycket om, asså när man pratar om financial impact, det är alltid i en kontext. Och, eller financial impact, det är en av de impacterna som vi

		tittar på. Vi tittar på brand, på impact men också på det sociala och hur folk mår.
80.	Interviewee 1	Om medarbetare skulle må dåligt, skulle utsättas för en pandemi eller epidemi eller nånting och inte kunna jobba till exempel som är högaktuellt just nu så, ja, det är också en konsekvens. Folk mår dåligt av det, folk är sjuka och visst har det också en finansiell aspekt men det är framförallt viktigt att våra medarbetare mår bra och har det bra och att vi hittar alternativa sätt att arbeta så att de kan vara trygga och att vi kan få fram det vi levererar…, det vi ska leverera trots de nya arbetsprocesser och arbetsrutiner.
81.	Interviewee 1	Så låt säga cyberhotet, när vi mäter impacts, mäter vi inte bara det finansiella men det finns också som aspekt och det finns i alla våra analyser faktiskt. Ur ett data privacy och ett information security perspektiv så har vi en impact assessment som vi gör så fort vi utvecklar en ny produkt. Det vill säga en ny applikation eller köper en färdig tjänst eller en färdig applikation, SaaS-lösning eller cloud generellt. Alright, det var en svår fråga.
82.	Interviewer	Okej, fråga nummer 3 då. Does your organization have a risk management process tailored to mitigate and control cyber-threats? Hallå?
83.	Interviewee 1	Sorry, jag var tvungen att mute:a när jag skulle hosta.
84.	Interviewer	Ok, (skrattar)
85.	Interviewee 1	Men, så vi har en risk management process på plats och enligt vår risk universe så finns det (paus) hanterar vi säkerhet, så cybersecurity, digital security, data eller info, aah, data security o sånt inom ramverket, så det finns en visst en uppföljning. Och hotet är en aspekt av risken.
86.	Interviewee 1	Det beror på vem man pratar om risk med. Om man pratar med business stakeholders så handlar risken väldigt mycket om, som i tidigare fråga, effekt och sannolikhet, så impact och konsekvens. *Impact och konsekvens, det är samma sak* (tänker). O probability. Impact o probability.
87.	Interviewee 1	O det, när man pratar med tekniska stakeholders så på application teams till exempel, så handlar det mycket mer om hot och sårbarhet så både impact och probability definierar en risk. Men också hot..., sårbarhet också definierar en risk men det är med olika stakeholders.

88.	Interviewee 1	O vi har ett internal control framework som jag nämnde i början så det är ett sätt o…, regler och hur man implementerar deras regler och vem är ansvarig för implementation och så vidare som används för att mitigera vissa risker. Så antingen är man medveten om en risk o då kan man lägga fram ett antal risker som vi vet åtgärder den risken. Eller gör man det på ett lite mer annorlunda sätt där vi gör en impact assessment som jag nämnde tidigare, där utifrån detta så får vi en klassificering för den applikationen och baserad på den klassificeringen samt kontexten till applikationen har vi ett antal åtgärder, relevanta åtgärder...
89.	Interviewee 1	Så mitigation finns i form av control framework och de är knutna till risker. Men kan liksom inte bara "mitigation för att bara mitigera cyber threats". Det finns i processen på nåt sätt. Den punkten skulle vi kunna utveckla lite mer. O det jag säger igen att vi kan (bryts) luta tillbaka till ett governance-modell det är för att det just förklarar den strukturen o form av regler men också den strukturen som (bryts) arkiv. Eller organisationen då som stödjer ramverket o implementationen av det ramverket. Så har man en puffig, fluffig risk management process som ingen förstår och ingen applicerar, det görs aldrig någon risk assessment o så, så är det onödigt. För att man kommer aldrig få veta om sina risker.
90.	Interviewee 1	Så det är viktigt att ha en process som stöds av en organisation och som förstås av organisationen. O det jag nämnde tidigare, det finns lite olika…, asså det finns olika stakeholders i en organisation, det finns de business inriktade människor som..., det är ingen idé att prata om dem om tekniska åtgärder eller cyber relaterade åtgärder för de måste ha en brandvägg eller de måste på något sätt logga access och sina transaktioner och så vidare. För att de har inte förståelse, nödvändigtvis för den tekniska delen.
91.	Interviewee 1	Däremot, har de fullt förståelse om andra aspekt som man kan fråga dem om. Och det kan vara relaterat till retention till exempel så de ska veta. En teknisk person inblandad i det tekniska teamet ska inte veta hur länge information kan bevaras eller få processas i en applikation. Däremot en business stakeholder ska kunna veta "ok men vi har kommit överens om hur information ska bevaras i 6 månader och efter detta så måste det raderas" till exempel. Eller vet de inte om det så är det bra tillfälle o lyfta upp frågan så att det definieras. På samma sätt, var ska den information host:as nånstans i världen, väldigt mycket av det som vi bygger eller (oljud i bakgrunden) nu för tiden.

92.	Interviewee 1	Så ligger det i cloud så finns det inte fysiska begränsningar som om det stod i våra data centers. Så det är inte så viktigt att veta om det bara finns i EU eller om det ska finnas i USA eller i asien och så där. Eftersom vi finns i många länder, mer än 30 stycken så finns det olika lagar som gäller i olika länder. Nu pratar vi om GDPR som var det första data privacy law och kom ut 2018 men bara i år hade det planerats att implementera någonting om 14 olika data privacy laws i världen. Både i Afrika, Sydamerika, i Asien o USA, Kalifornien. Så det blir mycket mer komplext.
93.	Interviewee 1	Det vill säga om vi kanske har en applikation som ska gälla för alla våra verksamheter i hela världen, vi kanske inte kan ha data som faktiskt är konsoliderat på ett och samma ställe. Data måste kanske finnas i Kina för Kina och i Ryssland för Ryssland och stanna i Europa för just Europa. Så det sätter begränsningar till vår business och en business stakeholder ska förstå dem kraven. De kraven relaterad till, location, retention, hur ofta man ska göra access reviews av sina accounts, alltså konton som finns i den digitala produkten och så vidare. Och om…, genom att göra en sån assessment gör man en bedömning om hur mogen är organisationen kring dessa frågor. Så har de inte förståelse för det så är den typ av assessment, asså data privacy assessment eller business impact assessment väldigt bra sätt o öka awareness.
94.	Interviewee 1	Med de tekniska teamen, de som antingen utvecklar eller implementerar det som är relevant för att diskutera kring kryptering, kring access control, kring segregation of duties, ehh (oljud i bakgrunden) o på samma sätt förstår de inte de kraven som appliceras på dem eller deras produkt. Så, det är också ett bra sätt att öka awareness kring detta. Både de krav som vi har dvs. lite mer softa krav som vår business har och de tekniska kraven som vi har för applikationen, produkten så är det en del av vår internal control framework som man ska se som en onion till exempel. Det finns ett yttre lager som är mer asså softa och strategiska krav. O ett inre lager som är detaljerad o sen ett nytt inre lager som är mycket mer detaljerad som kan handla om krav på algoritm o krav på protokoll och så vidare. Som appliceras till olika stakeholders då.
95.	Interviewee 1	Så, jag hoppas att jag kan knyta tillbaka till er fråga som handlar om risk management process och hur vi mitigate en control cyber threat. Ja det görs på olika nivåer. Det är inte nödvändigtvis hot vi pratar om. Ehh för businessen, så pratar vi mer om impact. Hur ska vi prata med tekniska stakeholders men allt detta handlar om att upplysa businessen om de riskerna eller hoten som finns och hitta en rimlig nivå, alltså

		säkerhetsnivå för att mitigera detta utan att förhindra businessen.
96.	Interviewee 1	Yes, och vi har ganska mycket kvar. För det känns som om vi skulle kunna fortsätta i en timme till.
97.	Interviewer	Kan vi?
98.	Interviewee 1	Fast nej, inte nu tyvärr, men kan vi passa på att boka en ny tid?
99.	Interviewer	Ja det kan vi göra.
100.	Interviewee 1	Kan jag avbryta inspelningen nu?
101.	Interviewer	Ja det kan du göra.
		PART 2
102.	Interviewee 1	Ok, så, bara för kontinuitet och för att uppdatera om vad vi har…, nu är det andra tillfället vi pratar med varandra och vi stannade förra gången med data breaching som sagt. Och nästa fråga, what do you know about the term data breaching?
103.	Interviewer	Precis, ja.
104.	Interviewee 1	Så, det finns lite olika dimensioner av det. Det ena ur ett legalt perspektiv, jag skulle säga. Exempelvis GDPR, så är det definierat som information som läcker i organisationen, oavsett om den har läckt ut avsiktligt eller oavsiktligt, om det var en attack eller om det var av negligence, eller om det är baserat på att man har bristande rutiner på plats, exempelvis skicka ut information okrypterat och man råkar bli avlyssnad på en kommunikation o sånt. O sen, förutom den legala definitionen så handlar det om vilken typ av data som helst egentligen, inte bara personuppgifter som råkar bli exponerad och utnyttjad av obehöriga (paus) så, ja. Förlorad information, antingen läckt ut eller (otydligt) eller att det finns en brist i processen eller chain of custody. Nästa fråga, ska jag hoppa över.
105.	Interviewer	Ja, yes.
106.	Interviewee 1	Innan dess, jag är faktiskt lite nyfiken och höra vad är er definition av data breach.
107.	Interviewer	Det är ju typ att data blir leaked till folk som inte ska ha den datan. (oljud utifrån)

108.	Interviewee 1	Förlåt du bröts. Jag ska stänga fönstret här också. Så vi inte har så mycket ljud utifrån, så, vad sa du, det sista.
109.	Interviewer	Vi har kanske inte en sån hära utförlig definition men typ en allmän är ju, data breach is an incident where information is stolen or taken from a system without knowledge or authorization of system owner.
110.	Interviewee 1	Är det den definition ni själva använder i er studie eller är det nånting som du precis hitta på internet?
111.	Interviewer	Nej, vi har skrivit det i texten.
112.	Interviewee 1	Ja, men jag kan nog hålla med er definition.
113.	Interviewer	Ja, vi ska typ undersöka hur, organizations, vad de har för issues och asså, inom just det området.
114.	Interviewee 1	Mm, ja. Fint. O sen är nästa fråga, relaterat till effekterna.
115.	Interviewer	Ja.
116.	Interviewee 1	Så jag skulle säga att vår risk management process definierar impacts case, och det finns 3 olika perspektiv för att definiera en impact. Så risk består av en impact o en sannolikhet för den impacten när den inträffas så den definierar själva risken ur ett business perspektiv. Impact i sig kan vara relaterat till…, asså en finansiell impact som ni beskriver. Det kan vara på brand och reputation. Det kan också vara på människor och businessen i sig. Om vi ser på människor, det kan vara människohälsa. Nu är vi mitt i en pandemi, där vissa beslut kan ha enorma konsekvenser på människors hälsa, människors produktivitet, för business outcome också. Så det är verkligen en relevant aspekt som (bryts) får uppleva sin fulla dimension, sin hela dimension just nu. Som…, jag skulle föreslå att ta hänsyn till också.
117.	Interviewer	Mm.
118.	Interviewee 1	O ni skriver asså from customer's perspective, from employee's perspective. Det är klart, om man pratar om reputation, det har en konsekvens på business. Men det handlar om människohälsa eller människors produktivitet, så är det en annan sak.
119.	Interviewee 1	Och en data breach skulle definitivt ha konsekvenser, möjligtvis på alla tre, asså finansiella konsekvenser i form av böter, i form av lost of

		confidence, så att kunder blir kanske inte så..., de blir tveksamma kring att handla på (organisation 1), eller handla online hos oss. Så det kan ha konsekvenser också, asså finansiella konsekvenser på så sätt.
120.	Interviewee 1	Och sen, visst är det alltid dåligt, bad will perspektiv, och reputation, asså rykte, det skulle skada vår image, vår brand. Nu är det så att, det finns olika sätt o agera. Det kanske kommer som fråga vidare, jag vet inte. Men om man tittar på dem stora data breaches som har varit, inom retail till exempel som Target, eller även inom banking i Sverige som Nordea som var target för phishing attack till exempel. De har lyckats kommunicera så pass bra så att de har vunnit, deras brand har vunnit att just detta om hur de har hanterat en sån kris och en sån situation. Så om man tittar på Target idag, de har investerat enormt mycket pengar för att hantera sin säkerhet ur ett top down, bottom up approach och systematiskt monitorera, övervaka, access:a, och så vidare. Så att det till och med har varit positiva effekt av det.
121.	Interviewee 1	Kortsiktigt så har det varit väldigt skadligt för företaget. Jag minns inte hur många, jag tror att det var typ 160 miljoner dollar som de förlorade på grund av den breachen. Så det är enormt mycket pengar. Men om man tänker på Target idag och deras rykte idag, jag tror inte att de längre drabbas av att de för några år sen, har haft en data breach men snarast att man ser dem idag som ett företag som har full koll på sin säkerhet. Så det finns…, det beror på helt hur man hanterar en sån situation tror jag. Hur bra man är på att kommunicera om just sina svagheter men också om sina åtgärder. Jag får hoppa till tredje frågan.
122.	Interviewer	Yes.
	Interviewee 1	Technology is constantly changing, what does your organization do to keep your system's quality high together with keeping employees and customers up to date. Det är en tricky question. Kan ni utveckla lite grann om vad ni menar där? Kan ni bryta ner frågan lite grann så det blir enklare för mig att svara, eller försöka.
123.	Interviewer	Ja vi tänker till exempel om ni använder er utav nån typ av system för att undvika såna attacks och hur ni liksom keep era employees and customers up to date. Om detta förändras, kanske inom något system.
124.	Interviewee 1	Ja, alright. Ja, men jag kan försöka svara på det. Det handlar inte så mycket om system i sig. Jag skulle säga att det handlar om våra applikationer i stort, samt supporting infrastructure. Så, asså vi har

		100-tals applikationer där ute, om inte 1000, eller flera tusen egentligen. Men de är av olika kritikalitet såklart. O baserat på den kritikaliteten som mäts, ur 3 olika perspektiv, asså konfidentialitet, integritet och tillgänglighet. Rate:ar vi dem 3 olika områden och det ger oss en klassificering och klassificeringens spegling ger kritikalitet för den lösningen. Baserat på klassificering så har vi olika krav som gäller och appliceras. Vi har en komplex kravmassa, så om vi tar helhet så har vi nånting som 488 krav totalt som appliceras för en produkt, en process och den organisationen som stödjer detta. Sen filtrerar man bort det som blir relevant baserad på klassificeringen så får man en viss antal krav.
125.	Interviewee 1	Vi har sammanfattat, eller tagit ut ett antal kontroller som vi kallar för "top 20 security controls". Så utifrån den kravmassan så har vi lyft upp 20 kontroller som vi tycker är högt relevanta för produkter, för applikationer. Och varje av dessa kontroller är riktade i form av CIA asså konfidentialitet, integritet, integrity o tillgänglighet, availability. Så klassificeringen gör en sån rating och då kan vi select:a utifrån de där 20 kontrollerna. De som är relevanta för att mitigera en sån impact som man har identifierat i business impact assessment, utan att behöva gå in för mycket i detalj då.
126.	Interviewee 1	Låt säga att kritikalitet översätts i ett antal kontroller och dessa kontroller monitorerar vi ur olika perspektiv. Det kan vara genom log analysis så allt som loggas inom applikationen, vad kan vi lära oss av detta. Det kan vara genom scanning av applikation, av nätverk, scanning av kod, discovery inom en databas till exempel. Dessa tester ger oss också indikation om hur de kontrollerna är implementerade, då topp 20 kontroller är implementerade.
127.	Interviewee 1	Men också genom att övervaka konfiguration av dessa kontroller som eventuellt är automatiska, i de operativ system, applikation, databas, infrastruktur och så vidare. Så detta ger oss 3 olika sätt och monitorera som vi kan göra kontinuerligt. Som sagt, konfiguration genom scanning och genom log analysis. Utöver detta så kan vi på ett lite mer intrusivt sätt assess:a kontroller, genom att ställa frågor. Vi kan ställa frågor till nån som är inom ett product team, så en applikationsteam som känner (paus), att de har lite mer kunskap inom säkerhet o privacy, som är kanske deras security champion. Sedan kan vi fråga den personen att verifiera konfiguration, kanske i en brandvägg, verifiera resultat av en pentest som har gjorts, gå leta efter specifika loggar och bevis för att säkerställa att en viss kontroll genomförs eller inte.

128.	Interviewee 1	Så det är ett sätt, att fråga nån insider inom produkt-teamet. Man kan också fråga business owner o den personen skulle kunna svara på vissa frågor om var den informationen som processas av applikationen skulle lagras nånstans, så var är det ok att lagra, asså är det ok att lagra det i Europa, i USA, i Kina, beroende på vem det är som använder den produkten o den lösningen. Så baserat på den informationen så kan vi sen, i form av discovery eller scanning identifiera var den informationen ligger och om vi är compliant.
129.	Interviewee 1	Vi skulle också kunna fråga product owner om (paus) när det var senaste gången det gjordes någon (otydligt) review till exempel, eller account review, var är retention period för informationen, och om det gallras i så fall om man tar bort den gamla informationen när den inte är relevant längre, och så vidare. Och sen en tredje typ av assessment som man kan göra är en full size audit. Så att man har en oberoende auditor som gör en full granskning, som tittar på alla kontroller, hämtar bevismaterial och gör sin bedömning då, om hur den är compliant till våra regler.
130.	Interviewee 1	Ok, ja förlåt att jag avbryter dig. Är detta något ni berättar för era liksom customers, och utbildar (paus), är det nåt ni utbildar era employeer inom, eller employees?
131.	Interviewee 1	Mm, o sen vad gäller, asså kommunikation mot våra kunder och mot våra medarbetare så är det en annan sak. Vi behöver inte kommunicera om vad vi har hittat för risker till exempel, eller för significant findings och så vidare. För att det vi vet om en produkt ska vi..., speciellt om det är en deviation ska vi åtgärda snarast.
132.	Interviewee 1	Men det finns sätt o kommunicera till exempel med våra customers genom (paus) asså varje gång en kund ansluter sig till vår webbsida till exempel så får de godkänna ett antal saker och då är det ett väldigt bra sätt att kommunicera med dem om vad de har för rättigheter och eventuella skyldigheter samt vad vi gör med deras data. Vad de har för rättigheter till exempel för att kunna fråga oss vad vi har för data om dem, asså det handlar väldigt mycket om individual rights i så fall. O vad de har rätt att fråga oss om, ja till exempel om de vill att vi ska ta bort den data vi har om dem eller andra åtgärder. Så detta är ett väldigt bra sätt att kommunicera med våra kunder om olika saker, både om cookies, om individual rights, det kan också vara om vår ethics policy.

133.	Interviewee 1	Och jag vet inte om ni har haft möjlighet att titta på vår senaste app som är lanserad i vissa marknader. Vi har flera, väldigt många möjligheter för kunderna att anonymisera sig när de söker efter produkter, eller ta bort anonymiseringen där de vill just att man håller spår på vad de tittar på o få förslag på saker där de kan anytime i appen bestämma att vi inte får spåra vad de gör framöver tills de ger oss tillstånd igen. Så det kan vara väldigt intressant att ha spår eller spårbarhet för en kund inne i appen eller webbsidan för att de vill gärna komma ihåg vad de har sett, om de like:a nånting. Då är det inte anonymt längre, det måste kunna knytas till deras profil.
134.	Interviewee 1	Så det där sättet att kommunicera med kunder och det har man möjligheter nuförtiden att göra det mycket mer interaktivt genom appar eller webbsidor och påminna dem om vad de har rätt till. Vad gäller våra coworkers, så employees, skulle jag säga att det fortfarande inte handlar så mycket om specifika applikationer för att kunna driva vår verksamhet och kunna hjälpa våra medarbetare med det de behöver till exempel performance review vad gäller, asså lön...information vi behöver om dem för att kunna betala ut till exempel lön. Vi behöver kunna behålla en viss segregation of duty så att vi vet att vem som helst inte kan få access till deras information. Jag skulle vilja förstärka att det inte är så mycket på applikationsnivå att man kommunicerar med våra medarbetare om säkerhetsåtgärder.
135.	Interviewee 1	Men skulle... (paus) asså jag försöker bara knyta tillbaka till den rubriken som handlar om data breaching. O frågan är inte specifikt data breach men handlar om hur vi skulle kommunicera med våra medarbetare om information läcker ut så finns det rutiner för detta. O de skulle få veta och vi skulle också behöva rapportera det till myndigheter om detta oavsett om det är customers eller coworkers så har vi skyldigheter på den nivån.
136.	Interviewee 1	Så hur arbetar vår organisation för att upptäcka, prevent och announcing data breach? Det är en bra fråga. Så det handlar om flera olika saker där. Upptäcka, jag pratade tidigare om continuous monitorering och continuous assessment, det skulle vara i så fall för att kunna upptäcka om en applikation inte följer våra krav o uppfyller våra krav. Så det handlar inte så mycket om detection men om just de kontrollerna som vi kräver inte finns på plats så finns det risk att vi skulle inte se ehh exempelvis en breach. Så det är mest proaktivt i så fall. Detective, så har vi ett antal kontroller implementerade i vår infrastruktur och våra

		applikationer i form av, som jag nämnde tidigare, log analysis, scanning, eventuell data loss och så vidare.
137.	Interviewee 1	Så skulle vi eventuellt detect:era att information rör sig på ett sätt som inte är godkänd. Och för att åtgärda då i så fall om man har detect:erat att information läcker ut så det är lite grann det jag pratade om tidigare. Det finns rutiner för att kommunicera med berörda utifall att personuppgifter har läckt ut, oavsett om de är kunder eller om de är medarbetare, och med myndigheter såklart. För att vi har skyldigheter att rapportera. Yes, nästa rubrik.
138.	Interviewer	Yes, vi tar den då.
139.	Interviewee 1	(läser upp frågan) Implementation of a plan and strategies concerning cyber security and cyber crime data breach perspective. Could you explain what plan or strategy(s) your organization has developed to combat cyber crime and prevent cyber-attacks such as data breaches. (paus) Låt mig (suck) fundera (paus). Så på strategisk nivå har vi flera olika movements som vi jobbar med aktivt för att förebygga, så prevent cyber attacks.
140.	Interviewee 1	Den ena handlar om security and privacy by design. Det innebär att vi vill att säkerhet och privacy åtgärder finns med i application life cycle från första början och genom hela utveckling och hela förvaltning, hela vägen till decomposing av en produkt.
141.	Interviewee 1	En annan movement som vi har i vår strategi handlar om kontinuitetsplanering. Som sagt vi (bryts) identifierar vad är det som är kritisk information, hur mycket av det behöver sparas, o hur länge. Om vi skulle behöva komma till en disaster recovery plan och aktivera en sån plan, hur mycket skulle behöva återställas och hur snabbt, för att kunna börja jobba igen så att teamet kan börja med sin applikation igen.
142.	Interviewee 1	Hur mycket data måste man återställa tillbaka i tiden, man kanske inte behöver återställa hela 10 års historiken, det kanske räcker med 1 månads historik för att komma igång men också identifiera var är de kritiska tidspunkter ehh för en applikation. Till exempel inför vissa helger, eller under vissa helger, inför jul till exempel när det finns kanske en specifik handel. Finns det vissa stunder då en applikation absolut inte vara nere, ska absolut inte krascha. Så business continuity planning som sagt är en annan movement.

143.	Interviewee 1	Third party security management ur ett strategisk perspektiv, det handlar om att ha lika bra kontroll över de applikationer vi har lagt ut hos partner, än de som vi har in-house. Så, som jag nämnde tidigare, genom att göra continuous monitoring, continuous assessment av dem där third parties och fourth parties och så vidare samt deras underleverantörer. Det finns en annan strategisk movement som handlar om civil trust och som handlar om att kunna styra mycket av säkerheten baserad på behörigheter och identiteter, istället för att lita på en infrastruktur, eller behöva lita på brandväggar, eller lita på vpn, och så vidare.
144.	Interviewee 1	Så för att kunna knyta allt tillbaka till identiteter. Vad ska en specifik användare ha rätt och se och i vilka omständigheter och så vidare. Så, dessa är några exempel av proaktiva åtgärder som vi har på ett strategisk perspektiv som nedbrutet och leder till många olika kapabiliteter och aktiviteter att genomföra, för att förebygga data breach bland annat.
145.	Interviewee 1	Has your organization had any data breach, external or internal, as a direct effect from your mitigation plan or strategy. Så, har vi haft data breach som en effekt av vår strategi?
146.	Interviewer	Vi menar kanske mest om ni har haft nån data breach, external eller internal.
147.	Interviewee 1	Det har varit fall där information har läckt ut som typ…(paus), som... vad heter det… (paus), inte tillåts enligt GDPR. Till exempel så har vi haft i ett land; information som vi har köpt genom nån marketing, third party. Gav information om vem, var användare. Så en användare kan logga in inom (organisation 1) webbsida till exempel så att alla artiklar som man klickar som favorit stannar och är knutna till just den användaren men också att man kan hantera sin productlist och allt sånt. Som leverans, veta om tillgänglighet i lager i närmaste varuhus eller där man brukar handla och så vidare.
148.	Interviewee 1	Ja, det har varit ett fall där information faktiskt har kommit med till en tredje part, som det inte skulle göra. Så vi fick veta det från den tredje parten och åtgärda det så fort som möjligt. Det är ett fall som jag vet om och det var precis innan GDPR kom i kraft. Men det..., ja, såna tillfällen kan hända och jag är inte medveten om såna breaches som har hänt sen efter maj 2018, då med skyldighet att rapportera till myndigheter.

149.	Interviewee 1	Jag vet ett fall där information har rapporterats eller en incident har rapporterats till myndigheter men det var en false positive dvs. det var ingen incident i sig. Det var inom line of business men den personen eller det teamet var inte medveten om att det faktiskt skulle gå på det sättet. Så att det var enligt procedurer. Så jag har tyvärr inte så mycket mer information och ge er kring detta, jag har inga fräscha exempel.
150.	Interviewee 1	Så nästa fråga, from a technological and a software point of view, can you elaborate on the technical reliability within the organization. Asså vi har, som i de flesta organisationer nånting som heter three lines of defense eller six (6) side principal. Det vill säga att det finns tactical layer som är i vårt fall cyber security unit som stödjer businessen med att implementera kontroll, monitorera över implementation av dessa kontroller, och ja, stödja dem på massa olika sätt.
151.	Interviewee 1	Sen har vi, i second line har vi min gruppering som är mer strategisk, som ger direktion som monitorerar den övergripande gällande implementation av informationssäkerhet och data privacy inom organisationen.
152.	Interviewee 1	Sen har vi den tredje linjen som är internal audit och de driver egen agenda, de rapporterar till board... så, styrelse inom flesta företag. Och deras roll är att ha en independent view och vad de har i scope. Så om deras scope är informationssäkerhet och data privacy så kan de göra en specifik granskning om detta och titta på hur vi arbetar då ur ett strategisk och taktisk samt operationell perspektiv. Sedan gäller det att komma fram med findings eller risker och då bearbetar vi dessa med dem. Så det vill säga att vi kommer med en åtgärdsplan för att åtgärda just de där avvikelser som har identifierats. Svaret på frågan?
153.	Interviewer	Mm, ja.
154.	Interviewee 1	Ok, nästa sektion, challenges concerning cyber crime in regard to information and cyber security, data breach and its challenges. How does your organization tackle the threats and challenges such as data breach. Så, som jag nämnde tidigare så... (paus), speciellt vad gäller security and privacy by design det vill säga att säkerställa att informationssäkerhet och data privacy finns inbyggd i varje fas av en application life cycle.
155.	Interviewee 1	När en applikation håller på att byggas eller byggs och det är oftast en kontinuerlig process för att det förändras hela tiden. Det är inte så att vi

		bygger en applikation och sen kör vi den aldrig. Det finns kontinuerlig förändringar, eventuella nya funktioner, nya features eller…(paus), som behöver utvecklas och så vidare. För varje significant change så ska vi faktiskt ha en assessment där, nån form av workshop som vi har med intressenter där vi gör nåt som kallas för (otydligt)
156.	Interviewee 1	Så vi tittar på den förändringen och hur den kan påverka hela applikationen och sina integrationer, o baserat på de potentiella hoten som har identifierats så kommer vi fram med ett antal åtgärder som också måste tas hänsyn till för att preventivt åtgärda... ja, potentiella data breach då i så fall, o så för att agera proaktivt.
157.	Interviewee 1	Så vi tittar på olika attack scenarios och så vidare, för att identifiera just hot och sånt. (läser upp frågan) Are there any issues that cannot be solved before a data breach has occurred, what proactive measures are taken? Ja, det är väldigt svårt att säga. Det är inte omöjligt, men ja, det är alltid en fråga om prioritet då i så fall. Asså är vissa åtgärder viktigare än andra åtgärder så ska de såklart prioriteras så att de åtgärdas först. Men ja, det är en väldigt bra fråga. Sen kommer vi i en sektion som är GDPR specifikt.
158.	Interviewee 1	(läser upp frågan) How does your organization work with GDPR, a. how does your organization manage personal data and information or your employees, how does your organization manage personal data and information of your customers?
159.	Interviewee 1	Det finns så…, många olika åtgärder. Låt säga att min organisation är strukturerad som jag nämnde tidigare och därför ser jag en koppling i three lines of defense där min business unit som handlar om informationssäkerhet och data privacy är där för att sätta krav så vi sitter och förvaltar policies och rules och så vidare, som dikterar hur man ska arbeta med informationssäkerhet samt data privacy. Sen har vi inom cyber security, som är en ganska stor avdelning hos oss som jobbar tactical, så har vi lite olika grupperingar.
160.	Interviewee 1	Vissa jobbar proaktivt med monitorering och så vidare. Vissa jobbar reaktivt med incident response till exempel. Andra jobbar med assessments så de gör granskningar, de kartlägger, de mappar och deras uppgift är att säkerställa att vi identifierar alla våra produkter, applikationer som processar personuppgifter. Om det handlar om medarbetare eller om det handlar om kunder.

161.	Interviewee 1	Säkerställa just också att alla rutiner och processer finns på plats för att jobba enligt lagen, är att rätt tekniska säkerhetskontroller också finns implementerade för att förebygga mot data breach. Så det vill säga att, ja, allt från kryptering, segregation of duties, användningar, våra identiteter, och hur vi gör det, patch management, (otydligt) management och så vidare. Så, med detta på plats så har vi en ganska bra overview om vad…, vad för system, vad för applikationer används för att processa våra coworker's uppgifter och data.
162.	Interviewee 1	Det är samma sak för våra customers data. Det är lite grann om hur vi implementerar GDPR bland annat, i vår organisation, med de där two lines of defense, och sen finns också third line of defense som är internal audits som jag nämnde tidigare, som kan och har haft och har kampanjer där dem just assess:ar. Det kan vara GDPR, eller data privacy stored, customer data eller hur vi hanterar detta inom organisationen genom internal audits.
163.	Interviewee 1	(Fortsätter till nästa fråga, läser upp) How does your organization work to ensure that your customers are aware of the organization authorizing their data? Som sagt vi har, med kunder, en fantastisk möjlighet att kunna kommunicera med dem genom appar och webbsidor och speciellt med de senaste versioner av mobile apps eller webbsidor så finns det mycket mer interaktion möjligt.
164.	Interviewee 1	Så man kan ha nästan en kontinuerlig dialog med kunder om deras data, vad vi gör med deras data. Vi är ett väldigt protagonist företag, asså vi säljer ingen data whatsoever till någon. Vi (bryts) tredje part, partners, som hjälper oss olika kommersiella perspektiv också för att antingen identifiera rätt kund att köra kampanj mot och så vidare men vi säljer ingen data till någon och vi delar data bara med våra partners som hjälper med möjligtvis specifika uppgifter. Så, vi är väldigt noggranna med att kommunicerar om detta också. Så jag hoppas att jag svarade på frågan.
165.	Interviewer	Ja.
166.	Interviewee 1	(läser upp frågan) Implementation of a plan and strategies concerning GDPR, what were the key factors your organization focused on when getting ready for the GDPR implementation? Det fanns ett GDPR projekt för att förbereda oss inför GDPR, med ganska många inblandade och de jobbade enligt olika workstreams. Jag har inte varit inblandad så jättemycket i det arbetet, förberedelsearbetet men det var ett ganska

		långt, ett långdraget projekt med många inblandade o väldigt noggrant utfört också. O i tätt kontakt med top management också, så att de alltid var uppdaterade om vad vår status var och vår current state.
167.	Interviewee 1	(Fortsätter till nästa fråga, läser upp frågan) Since the introduction of GDPR in 2018, what has changed in the way your organization handles data and information from employees and customers. Det är klart att det har blivit väldigt mycket striktare och sen dess har det varit många andra länder som har adopterat eller är på väg att adoptera… liknande lagar och regulationer. Så detta tvingar oss att jobba mycket mer strukturellt med den information, när vi hjälper vår business med att antingen skaffa en applikation, köpa eller bygga det själva så hjälper vi dem med att säkerställa just att information och data används (paus) för det ehh.. syfte som var annonserad från början. Att man har alltid godkännande från kunder för att kunna använda deras data och så vidare. Så, jag skulle säga att det har förändrats organisationen ganska mycket och det finns väldigt mycket assessments som görs, mycket awareness som görs, det finns förståelse också från vår business.
168.	Interviewee 1	Det har framförallt skapat en stor rädsla också, rädsla att göra fel, vilket gör att det har kommit väldigt många frågor från verksamheten om hur man skulle agera i vissa situation och så vidare, för att folk inte vill göra fel och vill inte exponera företaget och branden i onödan. Så det är väldigt positiva effekt av GDPR.
169.	Interviewee 1	(Läser upp nästa fråga) Challenges concerning GDPR, is there any current challenges that your organization has to deal with concerning GDPR, so in regard to the implementation of the new GDPR laws? Så låt säga att det…, det finns alltid väldigt mycket att göra och vi har funnits väldigt länge så det vill säga också att vi har väldigt många applikationer som är gamla, långt innan GDPR eller andra privacy laws som man behövt anpassas som kanske finns inom nån backlog och så.. som behöver anpassas...
170.	Interviewee 1	Och de senaste förändringarna har varit mycket kring cookie-handling. Väldigt lite tid att göra förändringar egentligen. GDPR är en sak, man har kanske lite mer framförhållning. Det finns andra länder som har mycket mindre framförhållning, som till exempel Kina som kommer med liknande krav, eller motsvarande krav och som kanske ger ett par månader att anpassa sig, anpassa sin verksamhet till lagen o inte ett par år som Europa brukar ge. Lite förändringar och implementationer av nya förordningar eller regulationer.

171.	Interviewee 1	Nästa fråga handlar om, any previous challenges. Possible future challenges. Asså det handlar alltid om de här catch-up lek på nåt sätt. Asså det finns alltid förändringar som kommer det hållet. Och vi har som sagt en enorm legacy i form av applikationer, digitala produkter osv.. Så det gör det till en challenge och kunna migrera till nya anpassade produkter i tid. Oftast är det väldigt bra opportunity också för att det ger oss tillfälle och förändras och kanske decommission applikationer som annars hade säkert används för många år framöver.
172.	Interviewee 1	Trots att de kanske inte uppfyller exakt de behoven som vi har längre. Vi hade ingen anledning och bekosta en förändring i så fall. Nu, med den typ av krav på oss så motiverar det väldigt mycket för att kunna bevara compliant, förändringsarbetet. Så jag skulle säga att det är positiva effekt av detta. Ja, utmaningar såklart men, tillfälle, opportunities. Ja, vill ni på nåt sätt avsluta?
173.	Interviewer	Ja, om har du nån feedback? Nått annat du vill tillägga? (bryts)
174.	Interviewee 1	Som jag nämnde till er tidigare så finns det väldigt många relevanta frågor, i er frågebatteri. Jag skulle kunna rekommendera att man tittar på helhetsperspektivet och sen bryta ner detta i olika lager men att titta på övergripande, asså de compliance och risk perspektivet och vad, i samband med det strategiska perspektivet. Vad ger detta i form av operationella krav och taktiska krav? och hur detta bryts ned i organisationen. Så lite mer ur ett governance approach. Men jag hoppas annars att jag kunnat besvara era frågor och att det ger värde till det arbete som ni genomför. Absolut, det har varit väldigt bra svar. Väldigt utvecklande svar. Skulle ni ha frågor i efterhand, nånting som ni har inte begripit bland mina svar eller nånting som ni vill att jag ska utveckla vidare så får ni gärna återkomma.
175.	Interviewer	Får vi lov att använda er department name i uppsatsen?
176.	Interviewee 1	Förlåt, vad sa du?
177.	Interviewer	Använda er department name i uppsatsen, asså vilken avdelning ni jobbar på.
178.	Interviewee 1	Yup, jag jobbar på en avdelning som heter Group information security and data privacy.
179.	Interviewer	Det är ok att vi använder det namnet?

180.	Interviewee 1	Ja, absolut. Det går bra att använda namnet.

Appendix 4 - Handwritten notes from interview 2 [Int 2]

Interviewee: Interviewee 2 (Anonymous)

Interviewers: Sarah Shahid and Emelie Huang

Date of interview: April 28th 2020

Location of interview: Online plattform (Microsoft Teams)

Line	Person	Questions and answers
1.	Interviewer	Permission to record the interview then thereafter transcribe the conversation.
2.	Interviewee 2	"Ok." (försöker spela in, men fungerar inte) Förklarar att det beror på att

		företaget är väldigt strikta med säkerheten. Därför kommer intervjun inte att spelas in. Däremot får vi lov att skriva ner allt förhand.
3.	Interviewer	Asking if the interviewee wants to stay anonymous or if he/she will allow his/her name and title to be mentioned in the research?
4.	Interviewee 2	"Gärna anonym."
5.	Interviewer	Inform the interviewee that: the material gathered from the interview will solely be used for the research purpose and the publication of a BSc thesis, bara studie.
6.	Interviewee 2	"Ja ok."
7.	Interviewer	The interviewee can choose to cancel the interview at any time.
8.	Interviewee 2	"Ja. perfekt."
9.	Interviewer	Are the statements mentioned above accepted by the interviewee?
10.	Interviewee 2	"Ja." (men med tanken att vi håller personens identitet anonym)
11.	Interviewer	The interviewee will be informed that the completed research thesis will be sent to him/her if he/she wishes so
12.	Interviewee 2	"Jag tar gärna del av er studie, ska bli intressant att läsa."
13.	Interviewer	Vi presenterar vårt arbete (research question) och varför vi valt att skriva om säkerhet.
14.	Interviewee 2	Han tycker att vi har valt att skriva om ett relativt "hett" ämne som är viktigt idag. Finns potential för framtida jobb inom cyber security och security generellt.
15.	Interviewer	Tell us a little about you. What is your role within the organization?
16.	Interviewee 2	Är group Information Security Officer (ISO) som rapporterar till Chief Information Officer (CIO) i (organization 2). Först jobbade personen dock som konsult i mindre konsultbolag och KPMG med IT och riskhantering. Senare jobbade personen som Data Protection Officer (DPO) under 1 års tid inom loppet av GDPR implementationen.
17.	Interviewer	How long have you been working with this specific role?

18.	Interviewee 2	“Sedan 2018.”
19.	Interviewer	What background do you come from before you joined the organization?
20.	Interviewee 2	Revision, IT- management konsult och informationssäkerhet.
21.	Interviewer	What are your main responsibilities within the organization?
22.	Interviewee 2	Group information security officer. Jobbar med ledningssystem för informationssäkerhet, och jobbar bredare med flera säkerhetsområden. Bygger ledningssystemet för säkerhet. Konsult och var DPO (Data Protection Officer) från början (1 år) under GDPR införandet. Känner till personuppgiftshantering.
23.	Interviewer	Something that signifies your organization and department? How would you explain and define your organization’s and department’s working environment?
24.	Interviewee 2	Stor organisation med 25 000 anställda, följer en decentraliserad affärsmodell, unikt och erbjuder olika produkter. Skapar energi vilket innebär jättehög säkerhet. Diverse typer av energi transporteras och ges till slutkunden. Verksamheten är organiserad i 6 stora affärsområden med olika krav på säkerhet. Miljoner kunder och många personuppgifter som ska hanteras samt anställas.
25.	Interviewer	How can a typical workday look like for you?
26.	Interviewee 2	Väldigt varierande, 8-16 jobb är det inte, gör inte samma sak varje dag. Oftast är det projekt. Styr mycket av sin tid själv, flexibla arbetsdagar.
27.	Interviewee 2	What does Cyber Crime entail for you? What does Cyber Security entail for you?
28.	Interviewee 2	Begreppet cyber är rätt roligt enligt Interviewee 2. “Informationssäkerhet, säkrar hur vi hanterar vår information och data. Handlar om att skydda vår verksamhet i den digitala världen.” cyber crime - attacker som sker genom digitala världen, typer av cyber criminals, mindre (ex. gymnasieelever som är nyfikna) och större. “cyber security är inget nytt men är viktigt och något vi bör tänka på. cyber är det som händer i den digitala världen. Informationssäkerhet kan vara skydd av fysiska papper också. Traditionell säkerhet jämfört med

		cyber security.”
29.	Interviewee 2	(läser upp frågan) Does your organization separate the risk types into categories? Such as Internal and External risks, and if so, how are these managed?
30.	Interviewee 2	“Ja, en av liksom grundstenarna är att det måste vara riskbaserad. Riskanalys är grunden.”
31.	Interviewee 2	Stor sannolikhet att något kan hända därför finns både interna och externa (ex. pandemi) hot och risker. Operational risker (interna) viktigt att man vet hur man ska hantera en situation som t.ex covid-19. Finns ex. vissa i personalen som inte alls får bli sjuka. Har miljömässiga risker också, och antagoniska risker.
32.	Interviewee 2	Ny lagstiftning, alltså GDPR, vad betyder detta, data breach kopplad till GDPR, vilka konsekvenser man kan få av ex. en breach. GDPR berör alla deras affärsområden.
33.	Interviewee 2	(läser upp frågan) What are the financial effects of Cyber-threats and the risks that follow? “Svårt att sätta prislapp och vara exakt när det kommer till riskhantering. Men det är bara gissningar i slutändan.” Bolag med intrång har haft en påverkan på deras aktie, men det brukar gå upp igen. Vite och böter, kan inte erbjuda den tjänsten (tillståndet tas ifrån dem). Finns definitivt finansiella kostnader.
34.	Interviewee 2	Ryktemässigt och brand också. Påverkar allmänhetens bild av bolaget. Från anställdas perspektiv också - kan lita på att bolaget tar väl hand om deras uppgifter, att deras integritets bibehålls. På grund av att djupa säkerhetsintervjuer görs (på anställda) ex. drogtester.
35.	Interviewee 2	(läser upp frågan) Technology is constantly changing, what does your organization do to keep your System’s Quality high together with keeping employees and customers up to date? (Förstår inte riktigt frågan, vill att vi ska förklara och utveckla).
36.	Interviewer	Förklarar att det är en teknisk fråga och handla om den tekniska aspekten gällande säkerhet.
37.	Interviewee 2	Krav på säkerhet när man installerar nya system, gör riskanalyser så att rätt system implementeras. För system med känsliga uppgifter har man högre krav, ex. lösenord, fingeravtryck, osv. Helt enkelt riskbaserat. Mindre känsliga system som ex. inte har personuppgifter behöver inget

		lösen eller ett kort lösen.
38.	Interviewee 2	Händer att man gör fel också.. förmåga att kunna hitta fel i våra system. Upptäcks hela tiden sårbarheter i våra system. Security operations center (SOC) som monitorerar detta här.
39.	Interviewee 2	Vad gäller anställda: Bra processer på plats, de gör fel och en stor källa för risk ett eget program som jobbar med security awareness av anställda. E-learning, föreläsningar, artiklar på intranät om säkerhet. (utbildar dem), testar sina anställda genom att skicka ut länkar till dem som leder till nåt dåligt. Fokuserar och jobbar kontinuerligt med sina anställda. Information om säkerhet är viktigt att få ut (till anställda). Ett lekfullt sätt som gör att anställda lär sig om säkerhet. Så att man ex. inte lämnar ut uppgifter som man inte borde ha gjort.
40.	Interviewee 2	Noga med att kommunicera med sina kunder. Ser till att deras uppgifter är säkra och att de inte ska dela sina uppgifter med någon annan, att de byter lösen med jämna mellanrum.
41.	Interviewee 2	(läser upp frågan) How does the GDPR affect the way your organization works with detection, prevention and announcing a Data Breach? En stor omställning (GDPR). Måste rapportera så snabbt man upptäcker. Rapportering av data breach, ett stort krav pga. GDPR. Har 22h på sig att agera när nåt upptäcks. Vara tvungna att se till att alla anställda vet om vad som har skett, allt ska rapporteras till rätt person i organisationen (även det minsta lilla). Announcement, absolut, påverkar jättemycket. Prevention ser till att vi får ett systematisk arbete med Information Security (IS). Detection - förstärka och monitorering, arbete med Security operations center (SOC).
42.	Interviewee 2	(läser upp frågan) Could you explain what plan or strategy(s) your organization has developed to combat Cyber Crime and prevent Cyber-attacks such as data breaches? Nyckeln är att få till ett systematiskt och riskbaserad arbetssätt, mest kritiska process - (det är där de måste se till att det fungerar) Ha koll på vad som är viktigt och jobba riskbaserat när de jobbar med risksäkerhet.
43.	Interviewee 2	Veta vilka cyber criminals som finns, göra omvärldsbevakning och ha kontakt med myndighet, vilka hot vi bör spana efter, ex. ryssar, kineser och vad vår Security Operation Center (SOC) ska hålla uppsikt över. “Känn igen din motståndare är en viktig strategi.”

		Detect, prevent, announce - det är så de (organization 2) ser det gällande data breach. Enligt studie så tar det 36 månader innan man upptäcker det, efter det har inträffats. Bli bättre på att upptäcka är jätteviktigt.
44.	Interviewee 2	Sårbarheter leder till data breach. Vi identifierade sårbarheter, hittar sårbarheter i systemen, behörighetshantering är ett klassiskt problem. Viktigt att man arbetar systematiskt. Men det är bättre att hitta sårbarheter än att ha läckage.
45.	Interviewee 2	(läser upp frågan) From a technological and a software point of view, can you elaborate on the technical reliability within the organization? Att ha upptäcksförmågan är viktigt. Det Måste finnas ett behov för att skaffa säkerhet o liknande produkter och system, inte bara att någon säger att det är bra och att det är "inne". Teknik är jätteviktigt, men man tror att teknik kan lösa alla problem, men om man inte kan tolka eller visa resultatet har man inte så mycket fördel av det. Det ska finnas ett behov för ett system.
46.	Interviewee 2	(läser upp frågan) How does your organization tackle the threats and challenges, such as Data Breaches? Handlar om att känna till hoten and utmaningarna kopplad till det, kontinuerligt bevaka det, hela tiden bli bättre o ligga steget före. Behöver hålla jämna steg. Gäller att se till att vi har kompetens och personal som kan det. Att hitta kompetens är svårt för många inom branschen. Man lägger mycket tid på rekrytering.
47.	Interviewee 2	(läser upp frågan) Are there any issue(s) that cannot be solved before a Data Breach has occurred? What proactive measures are taken? Har grupp som bara arbetar med - First lines of defence, säkerhetsfrågor… olika roller i organisationen som hanterar olika saker och områden. Om vi pratar DB inom def. Av GDPR måste det hanteras direkt. Mycket folk som jobbar med säkerhet (first line of defence), sker en prioritering där.
48.	Interviewee 2	(läser upp frågan) How does your organization work with GDPR? How does your organization manage personal data and information of your *employees*? . GDPR projekt - noga med att se till att informationssäkerhet och dataskydd är en enhet och inte frikopplade projekt. Olika bolag gjorde olika vid implementeringen. GDPR innebär juridiska aspekter och tekniska aspekter och man ska kunna hantera båda.
49.	Interviewee 2	Dataskydds koordinationer ser till att man tänker rätt när det gäller

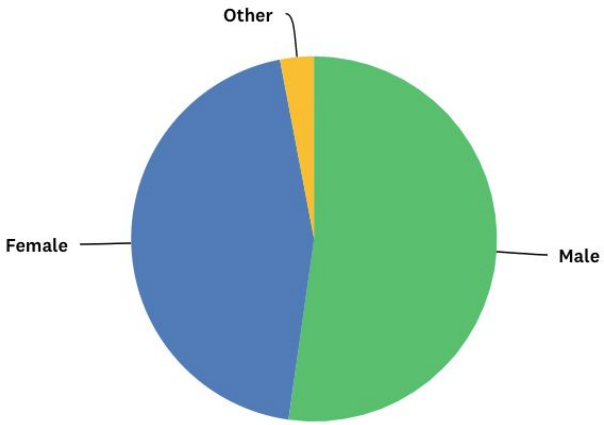
		dataskydd. På HR avdelningen har vi en dataskydds koordinator som vet hur uppgifter ska hanteras. Samma sak har försäljningsavdelningen, som vet hur kunddata ska hanteras. Anställda skriver ett kontrakt när man börjar jobba på företaget och vet vad företaget kommer använda anställdas personuppgifter till (ex. kunna betala lön).
50.	Interviewee 2	(läser upp frågan) How does your organization manage personal data and information of your customers? Betalningsuppgifter som kan vara känsligt. Har olika uppgifter beroende på om det är kunder eller anställda. Primärt hälsouppgifter (anställda). Stor del av arbetet de var tvungna att göra... se till att personuppgifter görs på ett transparent sätt.
51.	Interviewee 2	(läser upp frågan) How does your organization work to ensure that your customers are aware of the organization authorizing their data? “Privacy policy finns tillgängligt för kunder. Står tydligt om man vill kontakta företaget, hur man gör om man vill få personuppgifter raderade. Har inte en lång roman, (som oftast är långa texter), listar vad som är viktigt och har “om ni vill läsa mer…”. Man får sätta sig i kundernas perspektiv.”
52.	Interviewee 2	(läser upp frågan) What were the key factors your organization focused on when getting ready for the GDPR implementation? Hur hanterar vi personuppgifter, se till att rätt och uppdaterad information är stor del av arbetet, ha koll på, lägga mycket jobb på det (GDPR). Information och koll på behandling och utbildning på anställda, hur de ska hantera och rapportera en data breach la de mycket tid och jobb på. Se till att underleverantörer som hanterar information/uppgifter åt dem vet om sina skyldigheter. 3000 leverantörer, många av dem hanterar personuppgifter men de (organization 2) är fortfarande ansvariga. Så se till att de vet om deras skyldigheter och vad de ska göra.
53.	Interviewee 2	Viktigt att tidigt i projektet ta in privacy aspekten. Att bara ta med nödvändiga uppgifter och information. Detta regleras i biträdesavtalet.
54.	Interviewee 2	(läser upp frågan) Since the introduction of GDPR in 2018, what has changed in the way your organization handles data and information from employees? Customers? Nu tänker man före. GDPR fick en positiv effekt på hela säkerhetsarbetet, gjorde att anställda blev mer medvetna om säkerhetsrisker. En kultur som är mer medveten, de är mycket mer medvetna om hur man bör hantera uppgifter, skickar inte ut excel-filer som innehåller personuppgifter utan att tänka efter (nu de är bra på att tänka innan istället för efter), positiv förändring. Inte så stor förändring, förutom medvetenhet. 20 maj 2018, var en hysteri när det skulle införas.

		Men det var ju för att ingen visste vilka implikationer det blir. Rädd att göra fel - fick effekt som EU ville det skulle få, tror han.
55.	Interviewee 2	(läser upp frågan) Is there any current challenge(s) that your organization has to deal with concerning GDPR? Att hantera risker men inte gå för långt. För att enklare kunna utreda en breach vill man kunna spåra anställdas log och kolla deras mail men man vill inte gå för långt. Balansera olika lagstiftningar.
56.	Interviewee 2	(läser upp frågan) In regard to the implementation of the new GDPR laws? Ja, det finns det ju alltid. En sak som kan lyftas är kanske utmaningen som finns mellan olika lagstiftningar. Djupa kontroller av anställda, drogtester (tycker inte GDPR om), en konflikt mellan lagstiftningen i Sverige och GDPR. Det är en utmaning, alltså kunna balansera det här. (Olika lagstiftningar, integritet kontra säkerhet).
57.	Interviewee 2	(läser upp frågan) Any previous challenges(s)? Possible future challenge(s)? Olika länder med olika lagstiftningar, olika tolkningar i de olika länderna, finns fortfarande olika tolkningar i olika länder, olika regler som gäller i ex. Sverige och Tyskland. Finns länder där facket måste vara med och godkänna.
58.	Interviewee 2	Man blir aldrig klar. Kontinuerligt, måste fortsätta, orkar hålla i, se till att organisationen fortfarande följer. Bygger processer kontinuerligt.
59.	Interviewer	Do you have any other comments or feedback that you want to contribute with?
60.	Interviewee 2	Spännande område att jobba i, fler utmaningar i framtiden. Allt blir mer o mer ihopkopplade idag. Mycket möjligheter med digitalisering men riskerna ökar också. InfoSec blir ännu mera viktigt.
61.	Interviewer	Har en fråga bara, vad heter er avdelning?
62.	Interviewee 2	Corporate Security
63.	Interviewer	Får vi använda namnet på avdelningen i uppsatsen?
64.	Interviewee 2	Ja, det går bra. Men ska inte kunna spåras tillbaka till organisationen.
65.	Interviewer	Ja, det förstår vi.

Appendix 5 - Survey results

Gender

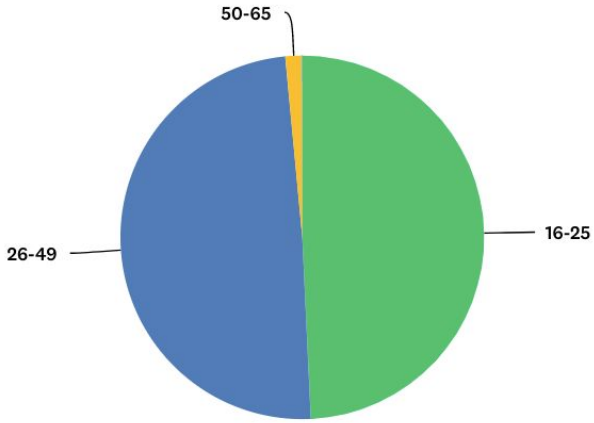
Answered: 67 Skipped: 0



SVARSVAL	SVAR	
Male	52,24%	35
Female	44,78%	30
Other	2,99%	2
TOTALT		67

Age

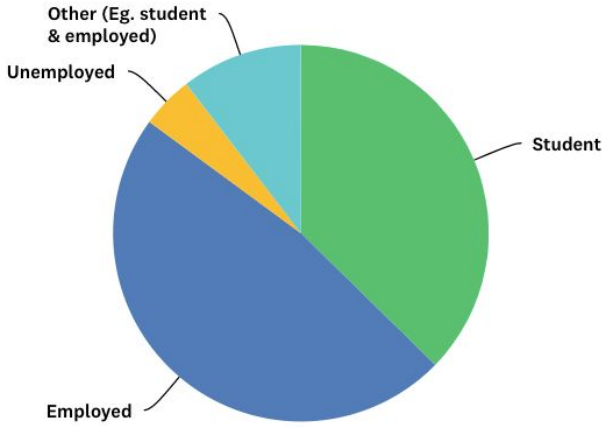
Answered: 67 Skipped: 0



SVARSVAL	SVAR	
16-25	49,25%	33
26-49	49,25%	33
50-65	1,49%	1
Over 65	0,00%	0
TOTALT		67

Occupation

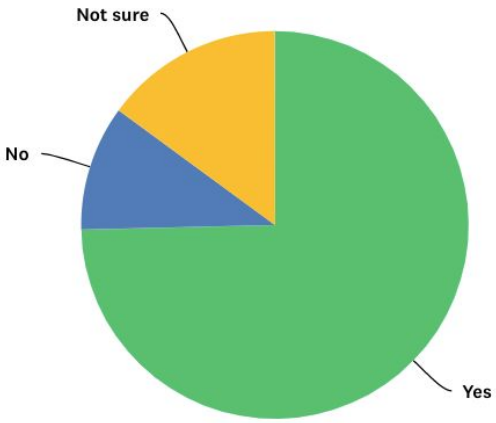
Answered: 67 Skipped: 0



SVARSVAL		SVAR	
Student		37,31%	25
Employed		47,76%	32
Unemployed		4,48%	3
Other (Eg. student & employed)	Svar	10,45%	7
TOTALT			67

Are you aware of data breaching* (leakage) issues within organizations?

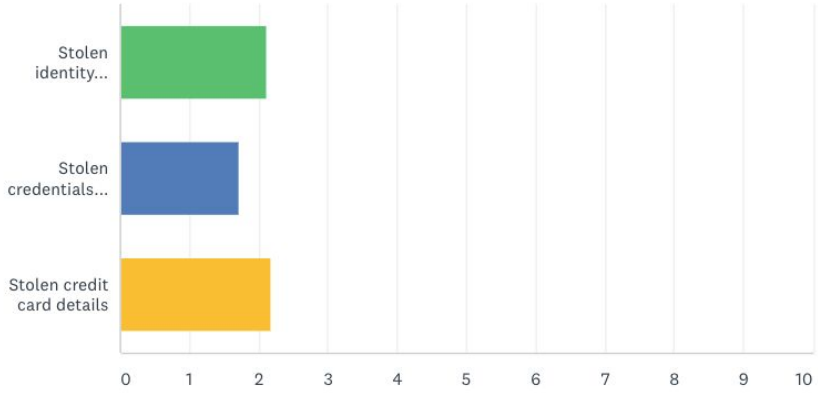
Answered: 67 Skipped: 0



SVARSVAL	SVAR	
Yes	74,63%	50
No	10,45%	7
Not sure	14,93%	10
TOTALT		67

If yes, which of the following data breaching* (leakage) issues concerns you the most? (rank them in order of most concern)

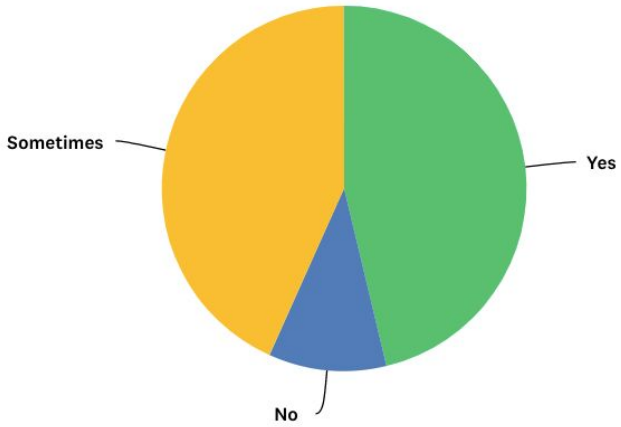
Answered: 58 Skipped: 9



	1	2	3	TOTALT	SCORE
Stolen identity information	37,93% 22	36,21% 21	25,86% 15	58	2,12
Stolen credentials (username/password)	20,69% 12	29,31% 17	50,00% 29	58	1,71
Stolen credit card details	41,38% 24	34,48% 20	24,14% 14	58	2,17

Have you ever thought about how your personal data is being handled by organizations?

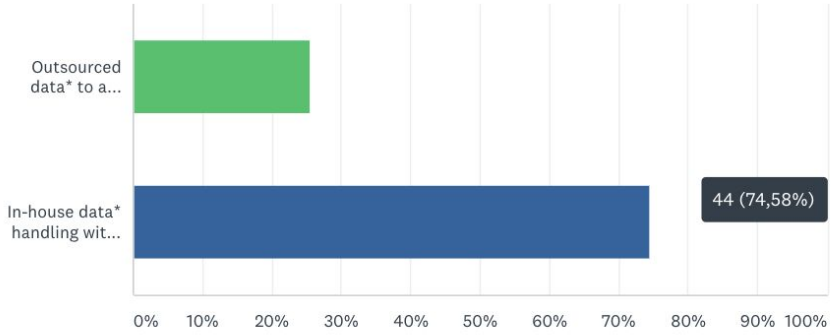
Answered: 67 Skipped: 0



SVARSVAL	SVAR	
Yes	46,27%	31
No	10,45%	7
Sometimes	43,28%	29
Not sure	0,00%	0
TOTALT		67

If yes, which data handling procedure would make you feel the safest:

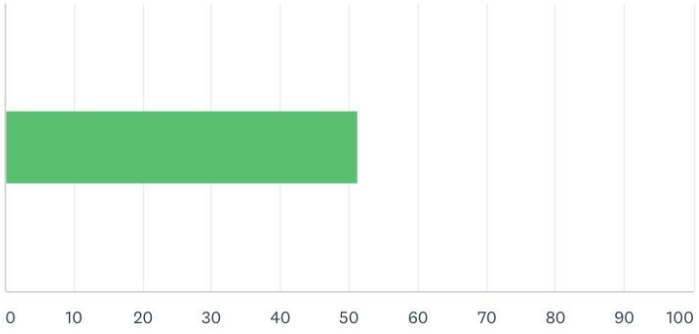
Answered: 59 Skipped: 8



SVARSVAL	SVAR	
Outsourced data* to a third party with known reputation	25,42%	15
In-house data* handling with latest technology	74,58%	44
TOTALT		**59**

To what extent are you concerned that your personal data can be leaked due to for instance cyber attack(s)* or technological errors within organizations?

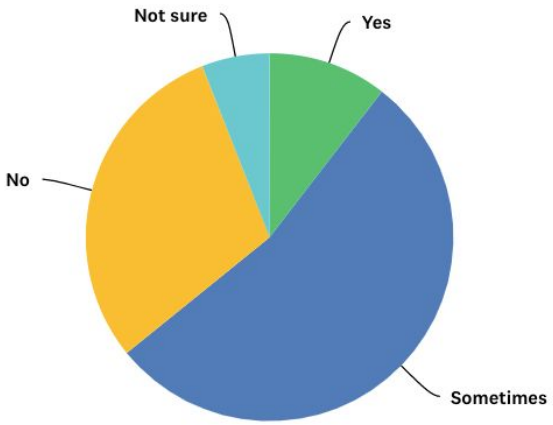
Answered: 67 Skipped: 0



SVARSVAL	MEDELTAL	TOTALT	SVAR
Svar	51	3 436	67
Totalt antal svarande: 67			

Do you think that organizations handling your personal data gives you enough information about how they authorize your data?

Answered: 67 Skipped: 0



SVARSVAL	SVAR	
Yes	10,45%	7
Sometimes	53,73%	36
No	29,85%	20
Not sure	5,97%	4
TOTALT		67