“The Cyber War”
A Qualitative Study Investigating the Management of Cybersecurity in Swedish Online Fashion Companies

Thesis for Master, 30 ECTS
Textile Management

Kajsa Steinbernreiter

Thesis number: 2018.7.01
Title: “The Cyber War” - A Qualitative Study Investigating the Management of Cybersecurity in Swedish Online Fashion Companies

Publication year: 2018

Author: Kajsa Steinbernreiter

Supervisor: Jonas Larsson

Abstract: Due to a world-wide digitalisation, the fashion segment has experienced a shift from offline to online shopping. Consequently, more companies choose to interconnect digitally with consumers and suppliers. This highlights cyber risks and cybersecurity issues more than ever, which becomes specifically apparent amongst online companies. Through qualitative semi-structured interviews with three different Swedish online fashion companies, the purpose of investigating how cybersecurity currently is prioritised and managed was reached. In addition to this, two cybersecurity experts gave their view of the most important aspects in the field, which companies should consider. Results showed a fairly well-managed cybersecurity amongst Swedish online fashion companies, even though knowledge in the field is scarce. Through educating everyone at the company and implementing a group of people in charge of these questions, a more holistic view could be attained. By offering thoughts on how online fashion companies can enhance their current cybersecurity, this paper contributes to the literature of cyber risk management as well as provides meaningful knowledge to all types of online companies.

Keywords: cybersecurity, cyber risk management, risk management, cyber risks, online fashion companies, fashion online, qualitative, Swedish, textile management
Thank you!

I would like to start by thanking the Swedish School of Textiles in Borås for giving me the opportunity of studying a two-year master in Textile value chain management. It has been a great experience.

Additionally, a big thank you to the three online fashion companies for your friendly help with this thesis. A special thanks to the interviewees for help and dedication during the interviews. It has been a pleasure interviewing you! Thank you to Ulf Gustafsson from PrimeSafe and Swedish police superintendent and head of frauds Magnus Lindegren too, for assisting me with great answers to my questions.

Jonas Larsson, I would like to thank you for your patience and guidance through this process. I would also like to thank my opposition group for great advice and help along the way.

Finally, I would like to thank my family and my friends, for always supporting me and believing in me.

Borås, 22nd of May 2018

Kajsa Steinbernreiter
List of content

1. Introduction 5
   1.1 Background 5
   1.2 Problem discussion 6
   1.3 Purpose 9
   1.4 Research questions 9

2. Conceptual framework 10
   2.1 Risk management 10
   2.2 Cyber risk management and cyber threats 11
   2.3 Cybersecurity 13
   2.4 The cyber risk management process 14
      2.4.1.1 Risk identification 14
      2.4.1.2 Risk assessment and valuation 15
      2.4.1.3 Risk response 16
      2.4.1.4 Risk control 17
      2.4.1.5 Risk culture and risk government 17
      2.4.1.6 To summarize 17
   2.5 Summary of the conceptual framework 19

3. Methodology chapter 23
   3.1 Research strategy: Qualitative research 23
      3.1.1 Criticism towards the chosen research strategy 24
   3.2 Research design: a case study 26
      3.2.1 Criticism towards the chosen research design 27
   3.3 Data collection method: semi-structured interviews 28
      3.3.1 Criticism towards the chosen data collection method 29
   3.4 Interview guide 30
      3.4.1 How the interviews were conducted 31
         3.4.1.1 Company 1 and Company 2 31
         3.4.1.2 Company 3 32
         3.4.1.3 Police superintendent and head of frauds Magnus Lindegren and co-partner of PrimeSafe Ulf Gustafsson 33
   3.5 Operationalization for the online fashion companies 34
   3.6 Operationalization for the cybersecurity experts 35
   3.7 Method of data analysis: qualitative content analysis 36
   3.8 Ethical issues 37
   3.9 Sampling 38
   3.10 Quality criteria 39
   3.11 Summary of the methodology chapter 40

4. Results 43
   4.1 Results from the online fashion companies 43
4.1.1 Company 1 43
4.1.2 Company 2 46
4.1.3 Company 3 50
4.2 Results from experts Ulf Gustafsson and Magnus Lindegren 52
   4.2.1 Ulf Gustafsson, PrimeSafe 52
   4.2.2 Magnus Lindegren, Swedish police superintendent and head of frauds 54

5. Analysis & Discussion 57
   1. Risk identification 57
   2. Risk assessment and valuation 59
   3. Risk response 61
   4. Risk control 62
   5. Risk culture and risk government 62

6. Conclusions & Future research 65

7. Managerial implications 66

List of references 67

Appendix 1: The interview guide for online fashion companies, step by step 74

Appendix 2: The interview guide for cybersecurity experts, step by step 77
1. Introduction

In this chapter, a thorough background to the subject of this thesis will be presented, together with a discussion raising questions about management of cybersecurity risks in an online fashion company. In the end, the purpose of the study and the research questions can be found. Finally, delimitations will narrow down the research even more.

1.1 Background

The fashion segment has experienced a shift from offline to online shopping, where companies operating online, i.e. online companies, offer fashion products online instead of in stores (Statista, 2016). Online shopping has increased during the latter years and is estimated to continue growing (Turban et al., 2017), which is a result of the world’s rapid digitalisation (McKinsey & Company, 2016; Griffor, 2017). Actually, Statista (2016) estimated online fashion to grow with a rate of 13.8% by 2021. Furthermore, Aaron Orendorff explained in Shopify (2018), that the online fashion industry will have a worldwide revenue of $713 billion US dollars by 2022. Even though huge opportunities arise with the digitalisation and the Internet, new types of risks emerge as well. These are defined as cyber risks (Refsdal et al., 2015; Griffor, 2017). Cyber is an abbreviation for cyberspace and includes all the different digital networks, such as the Internet, required for modification, storage and communication of information (Kosub, 2015; Refsdal et al., 2015). Today, the Internet provides unhindered connectivity, creating possibilities for interaction in numerous ways. Results from this open connection are often very beneficial, but sometimes also acts as a potential source for harm to a person or a property (Griffor, 2017). In order to protect against harm and hazards, managing of risks are not only important, but vital. Thus, most organisations are today involved in different kinds of risk management (Refsdal et al., 2015).

Risk management can be described as a process, where coordinated activities are implemented in order to protect the organisation from different risks (Refsdal et al., 2015). Waters (2011) explains that when implementing risk management, the company is prepared to deal with unforeseen events. One specific form of risk management is cyber risk management, which is necessary in an increasingly digital world, where more and more companies interconnect technology as well as digital environments with customers and
suppliers, in order to collect, analyse and work with huge amounts of sensitive data every day (Refsdal et al., 2015; Griffor, 2017). As part of cyber risk management, cybersecurity can be described as protecting cyber systems against cyber threats, which refers to the protection of information or infrastructure (Refsdal et al., 2015). Thus, cybersecurity is necessary when protecting company systems and cyber risk management refers to the overall cyber risk operations performed at the company. According to Griffor (2017), cybersecurity issues are reshaping value chains all over the world, as companies are integrating cybersecurity capabilities, making them an important part of sourcing decisions and in contractual terms of how their data should be handled. Kosub (2015) further stress cybersecurity to be specifically important for companies operating online, since these have greater cyber risk exposure. This is underlined by Kate Abnett (2016), writer for the journal Business Of Fashion, as well, who mentions online companies to be particularly at risk, since their entire business more or less can be found online. For instance, in 2015, Patagonia experienced a hacker attack on their website, where up to 12 500 customers got personal information stolen, whereof 600 customers’ credit and debit card details were compromised (Sturmer, 2015). Additionally, in 2017, Amazon was targeted by hackers, who used stolen credentials of Amazon-users, in order to post falsified ads and steal the received payments (The Wall Street Journal, 2017).

1.2 Problem discussion
As mentioned above, the digital world has increased a lot during the latter years (Griffor, 2017), where more or less everyone is relying on the Internet (Teplinsky, 2013). In 2020, it is estimated to be more than 50 billion active devices in the world (Serafin, 2018). According to Daniela Cecilio (2015), writer for the Guardian, the rise of online and mobile shopping is specifically relevant in the fashion industry. Not only individuals decide to go online, but also companies, where technology environments are increasingly connected with both suppliers and customers (Griffor, 2017; Serafin, 2018). Consequently, the change from traditional business models to Internet and digital business models increases both the number of potential cyber risks and the relevance of cyber risk management (Kosub, 2015). As the world becomes more digitized, it becomes more vulnerable, threats are expanded and intensified as well as online frauds are increasing (MacDonnell, 2014; 1). In fact, according to Swedish crime statistics agency BRÅ (2017), cyber related crimes increased by 39 percent

1 Magnus Lindegren, Swedish Police and head of frauds. Lecture at Ellos, Viared 7th of February 2018
from 2015 to 2016 in Sweden. This is mainly because of society’s increased and widely-spread Internet usage, but also because the digital development helps foster online frauds. Additionally, The Global Risk Management report listed cyberattacks as one of the top ten global risks during 2017, with a leap from place nine in 2015 to a place five in 2017 (aon.com, 2017). Despite this, cybersecurity sadly remains the area within risk management with the widest gap between the level of threat and the amount of resources invested (Khojasteh, 2018). In line with this, MacDonnell (2014) explains different cyber risks faced by companies to be growing, where most companies have limited current ability to protect against these. According to Griffór (2017), companies are facing risks not only with external attacks, with a goal to penetrate a system, but also with attackers existing on the inside of a system, and instead working their way out. Both MacDonnell (2014) and Griffór (2017) stress that far too many companies still do not understand or even ignore these threats and the importance of cybersecurity, which of course creates a lot of turbulence in the supply chain. Kosub (2015) and Rumsey (2016) additionally mention limited current knowledge about cyber risks and cyber risk management, which also jeopardizes companies’ ability to protect themselves.

Nevertheless, Griffór (2017) still underlines the fact that during the more recent years, most management teams and board of directors slowly have started to realize how much harm cyber attacks can do to their business. For instance, online fraud and other types of crimes can easily cost a company hundreds of millions of dollars. This is also stressed by MacDonnell (2014), who means that loss of product research and development as well as hundreds of millions of dollars in lost revenues are risks connected to cyber threats. Griffór (2017) continues to explain companies losing sensitive personal information to upset consumers, which could decrease revenues as well as bring the company legal problems. This is very damaging for the company’s reputation too (Kosub, 2015). If sensitive business plans get stolen, critical pricing, negotiation or blackmailing situations could occur. Perhaps most important, since most companies cannot function without daily access to core systems, an attack on these systems can close down the company for good (Griffór, 2017). Since all organisations are somehow exposed to risks, managing risks is vital for a company’s survival (Refsdal et al., 2015). In reference to cyber threats, any organisation can be targeted (Trautman, 2017). Actually, MacDonnell (2014) mentions two different types of companies:
those who have already been hacked and the ones unaware of it. According to the Swedish police superintendent and head of frauds Magnus Lindegren², an online fraud does not necessarily equal someone hacking into a company’s system. It might as well be an imposter sending an email with a fake invoice for the company to pay or an email requesting the company to “click on this link to update your company information!” for example. Emails like these are common for both companies and individuals, and yet it is not referred to as a “major risk”, even through it could be. The digital development fosters new crime possibilities, according to both BRÅ (2017) and Swedish police superintendent and head of frauds Magnus Lindegren³, which makes it difficult for companies and individuals to actually understand when being targeted.

Cyber threats have been called “the crime wave of the future” (MacDonnell, 2014, p.19), and reading all of the above, should make every company understand the benefits of implementing and upscaling cybersecurity. Companies becoming successful in this will not only reduce risks, but also increase organisational efficiency as well as improve their relationship with customers (MacDonnell, 2014; Griffor, 2017). Khojasteh (2018) further explains a robust cyber risk management to protect strategic goals, prevent business disruption as well as maintain company reputation. However, Kosub (2015) means that companies’ management of cyber risks needs considerable improvement and that a successful cyber risk management still is considered a challenge for companies.

The subject for this thesis is twofold. Firstly, since this type of study has not been applied to Swedish online fashion companies before and hence, a gap in the literature can be found, which needs to be filled. That could both help the said online fashion companies in practice as well as foster future research. Secondly, several researchers (MacDonnell, 2014; Kosub, 2015; Griffor, 2017) thoroughly describe the theoretical importance of managing cybersecurity and thus, it would be interesting to see if this actually is implemented in real companies, specifically Swedish online fashion companies.

² Magnus Lindegren, Swedish Police and head of frauds. Lecture at Ellos, Viared 7th of February 2018
³ Magnus Lindegren, Swedish Police and head of frauds. Lecture at Ellos, Viared 7th of February 2018
1.3 Purpose
The purpose of this study is to investigate how cybersecurity is managed in Swedish online fashion companies.

1.4 Research questions
RQ1: Is cybersecurity prioritised in Swedish online fashion companies? In that case, to what extent?
RQ2: How do Swedish online fashion companies handle cyber risks?
2. Conceptual framework

In order to highlight the theoretical gap of how cybersecurity risks are managed in Swedish online fashion companies, the conceptual framework will start by providing a general description of risk management, cyber risk management and cyber threats. The last part of the conceptual framework describes the cyber risk management process, which further on will serve as the basis for the results as well as the analysis and discussion.

2.1 Risk management

A risk can be described as the potential of something going wrong, which hence causes harm or loss (Refsdal et al., 2015). Waters (2011) defines risk in terms of unpleasant happenings that could occur and mentions risk in an organisation as a threat that needs to be protected against, in order to not disrupt any normal activities. According to Refsdal et al. (2015), the seriousness of a risk heavily depends on the likelihood of that risk occurring as well as the consequences it brings. Griffor (2017) instead explains the severity of a risk to be calculable, usually based on the perception of the potential loss and the likelihood of this harmful event happening again. Waters (2011) further describes risks to come in different forms and appear at any point in an organisation’s supply chain. Sometimes, a risk might just cause a small bump in the road and sometimes, the entire company collapses. This might further on solely affect one part of the supply chain, and in some cases, it threatens the whole chain.

Since all organisations are somehow exposed to risks, the management of risks is very important. Thus, risk management should be a part of the overall management of the entire organisation, to help and bring benefits to the business (Waters, 2011; Refsdal et al., 2015). Waters (2011) means that when implementing risk management, the company is prepared to deal with unforeseen events. As business is becoming more and more risky, with a growing number of risks facing the organisation, managing risks is more important than ever. Risk management is described by Refsdal et al. (2015) as a process, which “...comprises coordinated activities to direct and control an organization with regard to risk.” (p. 12). Moreover, Waters (2011) explains risk management as a process, where the organisation systematically identify, analyse and respond to risk. Khojasteh (2018) too describes risk
management to involve similar steps, and mentions risk identification, risk analysis, risk evaluation, risk treatment and risk monitoring.

Furthermore Waters (2011) explain two different ways for managers to react to risk: either ignore it or take a reactive approach. Commonly, companies ignore risks when these are “unlikely to happen”, in order to not waste any time on preparing for what probably will not happen anyway. If it does happen, though, companies often have back-up plans in order to respond accurately. The second choice, being reactive, is often too slow of an approach, where harm will be done even before the response takes place. In this approach, managers wait for the risk to occur, realize something has to be done, create the response, implement this and then wait for the recovery. Based on this, the author instead proposes a third, better approach: to identify any risk in advance and then prepare for the best response. This is similar to risk mitigation, mentioned by Khojasteh (2018), where strategies are implemented to reduce the likelihood of a risk occurring, as well as to decrease the negative impacts of said risk.

2.2 Cyber risk management and cyber threats

One type of risk management is cyber risk management, also called online risk management, which can be explained as the management of cyber risks (Refsdal et al., 2015; Griffór, 2017). Refsdal et al. (2015) mean that cyber risk management is closely related to risk management in general, but the risks are instead caused by cyber threats. These cyber threats can come from anywhere in the world, with the goal to cause damage and disruption inside a system (Kosub, 2015; Refsdal et al., 2015). Cyber risk incidents are increasingly common, which makes cyber risk management a necessity for today’s companies, in order to ensure stability and operability within the business (Kosub, 2015). Refsdal et al. (2015) further describe two different types of cyber threats: malicious and non-malicious. Malicious cyber threats are internal, while non-malicious cyber threats are considered external. Malicious threats could, for instance, be denial of service (DoS-threats), where intentional attacks are made. A denial of service attack is described by Techtarget.com (2016) as an event that occurs when a cyber attacker targets a specific system and prevents the rightful user from accessing this system. Non-malicious threats could instead be crashing systems due to
programming errors, for example, or loss of Internet connection because of faulty cables or hardware failure (Refsdal et al., 2015).

Cyber attacks are one type of cyber threat, which according to MacDonnell (2014) and Khojasteh (2018), often is an act of organized crime, such as fraud or identity and property theft. Cyber attacks can furthermore be divided up into espionage or sabotage, where espionage refers to illegal information retrieval and sabotage is described as intentional damage to IT-systems (Kosub, 2015). Cyber attacks is an upgoing trend amongst criminals and fraudsters, since it is easy for them to sit at home, by the computer, and blackmail companies into transferring money, for instance (MacDonnell, 2014; ⁴). Another example of cyber attacks could be website hijacking, which implies relatively low-risk for the attackers, who most often are from foreign countries and thus protected by this country's jurisdiction (MacDonnell, 2014). Cyber attacks are becoming increasingly costly for companies (Trautman, 2017), and can indeed be devastating. For instance, online frauds can cost hundreds of millions of dollars in lost business plans, research, knowledge, customers and future revenues. Additionally, a cyber attack on a core system, could easily shut down the entire company (Griffor, 2017).

There are different factors influencing today’s vulnerability in companies and their systems. First of all, the digital industry as a whole is vulnerable (MacDonnell, 2014). Since there is an ongoing change from traditional business models to digital business models, new, more complex challenges and risks arise accordingly (Kosub, 2015; Khojasteh, 2018). Additionally, cyber threats are considered a fairly new phenomenon, which creates a lot of ignorance amongst companies. Cyber threats are also expanding, and fraudsters become more and more intelligent and creative in their work (MacDonnell, 2014; ⁵). Overall, Kosub (2015) mentions current knowledge about cyber threats to limit companies’ ability to protect themselves. Rumsey (2016) agrees on this, and further mentions cyber threats to not be directly visible, which makes it difficult for companies to comprehend the severity. Thus, it is important to know that not enough companies, executive management and board of directors are aware of the problems created by cyber threats. Some companies even completely ignore

⁴ Magnus Lindegren, Swedish Police and head of fraud-section. Lecture at Ellos, Viared 7th of February 2018
⁵ Magnus Lindegren, Swedish Police and head of fraud-section. Lecture at Ellos, Viared 7th of February 2018
this, since the mindset more or less is “it will probably not happen to us anyway” (MacDonnell, 2014; ⁶). It is, however, important to realize that every single organisation can be targeted; no one is spared (Trautman, 2017). Thus, MacDonnell (2014) and Griffor (2017) further stress that managing cyber threats with the accompanied risks, creates increased competitiveness for the company, enhanced value for both the company and the consumers, new opportunities for the future as well as competitive advantage.

2.3 Cybersecurity

As part of cyber risk management, cybersecurity refers to the security of a system, in order to avoid a cyber threat (Refsdal et al, 2015). Kosub (2015) further describes cybersecurity as protecting any electronic information, the communication technology it depends on as well as the cyberspace-users. Basically, the protection of IT-systems and information within these systems. Refsdal et al. (2015) describe information security to be an important part of cybersecurity, in order to protect the electronic information a company might have. Thus, cybersecurity is necessary when protecting company systems and cyber risk management refers to the overall cyber risk operations performed at the company.

Griffor (2017) means that in an increasingly digital world, companies are using systems to interconnect with customers and suppliers, share business plans as well as collect and save huge amounts of data. This type of information is of course vital to secure and protect against cyber threats and unauthorized intruders. However, many companies do not prioritise cybersecurity due to lack of immediate threats, according to Kosub (2015), others simply just do not have the knowledge. Rumsey (2016) agrees on this and mentions companies’ lack of cybersecurity to be an immediate result of lack of knowledge. Trautman (2017) further explains board of directors, particularly in smaller companies, to have no engineering or technology training, which also leads to a lack of cybersecurity knowledge. Even though most companies currently do not prioritise cybersecurity as part of their company risk management (MacDonnell, 2014; Griffor, 2017; ⁷), it is hard to ignore the fact that cybersecurity concerns are reshaping and affecting value chains all over the world (Griffor,

---

⁶ Ulf Gustafsson, PrimeSafe. Lecture at Ellos, Viared 7th of February 2018
⁷ Ulf Gustafsson, PrimeSafe. Lecture at Ellos, Viared 7th of February 2018
2017). According to MacDonnell (2014), a company’s risk management is absolutely enhanced by the implementation of cybersecurity.

2.4 The cyber risk management process

Kosub (2015) identified a cyber risk management process with five steps: 1. Risk identification, 2. Risk assessment and valuation, 3. Risk response, 4. Risk control and 5. Risk culture and risk government. This process can be compared to Refsdal et al. (2015) process, which is called the Process for cyber risk assessment and contains five steps as well: 1. Context establishment for cyber risk, 2a. Identification of malicious cyber risks and 2b. Identification of non-malicious cyber risks, 3. Analysis of cyber risk, 4. Evaluation of cyber risk and 5. Treatment of cyber risk. According to Kosub (2015), a set of preventative measures together with risk transfer, is considered the most effective way of implementing cyber risk management. Refsdal et al. (2015) further mean that the implementation of this type of process, has a major impact on whether or not the overall cyber risk management will be successful.

The steps in Kosub (2015) process will serve as the base for this conceptual part, and thus be compared to Refsdal et al. (2015) process as well as other theory. All of the steps will be explained in detail below. Furthermore, Khojasteh (2018) stresses the fact that very few researchers address the theoretical frameworks of a risk management process connected to IT and cyber risks. Hence, the author explained the key steps of a general risk management process to possibly be adapted to IT and cyber risks. These will thus also be intertwined in the detailed explanations below.

2.4.1.1 Risk identification

In order to manage risks, these have to be identified. Thus, identification of cyber threats, which can turn into risks, is needed (Kosub, 2015). According to Waters (2011), risk identification is a process which helps reviewing uncertainties in a supply chain as well as list the most significant associated risks. Khojasteh (2018) too explains risk identification to involve the identification of a company’s key risks, preferably amongst all supply chain members. Both Kosub (2015) and Refsdal et al. (2015) further stress the importance of identifying valuable firm assets, which are vital for the company and thus might be
endangered by cyber threats. An asset is described by Refsdal et al. (2015), as anything valuable for someone. In this case, an asset could, for instance, be specific software. A correct asset identification is a key challenge for companies to properly assess cyber risks, according to Kosub (2015). In order to identify risks, Waters (2011) means it could be necessary to talk to knowledgeable personnel, the suppliers as well as outside consultants, for instance. If the company knows how cyber threats arise and which assets these might harm, Refsdal et al. (2015) explain, the company will also understand what needs to be protected and what risks are relevant to focus on. Risk identification as a first step, is specifically important for companies operating online, according to Kosub (2015), since these are more exposed to cyber risks and threats. Finally, a budget for IT security management should also be set at this point of the process (Khojasteh, 2018).

As a step two in Refsdal et al. (2015) process, identification of malicious respectively non-malicious cyber risks are implemented. This step can be seen as an extension of Kosub (2015) first step Risk identification. Refsdal et al. (2015) mean that it is important to understand whether the threat is intentional or not, in order to approach the threat in the right way. If the threat is malicious, the company needs to figure out who would want to initiate the attack, what the attack might exploit, what the intentions are and so on. If the threat instead is non-malicious, it is better if the company begins to look at assets instead of possible threat sources, in order to not get overwhelmed by how many potential non-malicious threat sources there might be.

2.4.1.2 Risk assessment and valuation

The company’s exposure to risk needs to be assessed and perhaps quantified. How much will the risk be worth in monetary units? There is a need to estimate possible losses as well as the likelihood of the identified cyber risks happening (Kosub, 2015), which is done in risk assessment and valuation. When analysing cyber risks, Waters (2011) and Refsdal et al. (2015) mean that it is important to estimate how likely it is for the identified cyber threats to occur, the consequences brought and how difficult it would be for the attackers to reach company assets. Management then need to decide if these risks are acceptable or if other measures need to be implemented (Kosub, 2015).
2.4.1.3. Risk response

After having identified the risks and calculated for their likelihood of happening, the best responses to the risks need to be selected and implemented. The best response usually depends on the significance of the risk, i.e. its potential impact (Waters, 2011). According to Kosub (2015), there are four different types of risk responses that can be applied: risk avoidance, risk mitigation, risk transfer or risk acceptance. In risk avoidance, the company avoids anything that could create a risk. In a cyber risk avoidance strategy, for instance, all or certain IT systems could be avoided. In risk avoidance as explained by Refsdal et al. (2015), it is sometimes necessary for the company to look for alternative solutions when being exposed to cyber risks. An example of this could be the change of computer systems.

In risk mitigation, preventive measures are taken in order to reduce the probability of specific types of cyber risks occurring. An example could be fire walls. However, these measures imply costs (Kosub, 2015). Investments in software solutions, such as fire walls, are referred to as risk prevention by Khojasteh (2018). In Refsdal et al. (2015) process, risk mitigation is instead referred to as risk reduction, where companies would want to reduce and eliminate as many threat sources as possible, and reduce the likelihood of a cyber risk to happen. However, the same authors mean that when it comes to malicious threats, it is close to impossible to eliminate the source of the threat. Kosub (2015) associates risk mitigation with costs and could be comparable to Refsdal et al. (2015) risk retention, which refers to the monetary costs of implementing and maintaining risk treatments.

In reference to risk transfer, it can be seen as an additional risk management tool, if the previous solutions should not be enough. Examples of this could be specialized cyber risk insurances, that cover losses from cyber attacks, or transferring risks to suppliers or customers (Kosub, 2015). Refsdal et al. (2015) explain this as risk sharing, where the company shares the risk through, for instance, insurance. This is instead referred to as risk mitigation by Khojasteh (2018).

Finally, risk acceptance can be implemented if the risks are not identified as relevant to the company, or if other risk response measures are too costly. However, it is important to know
that risks will never be entirely eliminated, which is most apparent in risk acceptance and risk mitigation (Kosub, 2015).

2.4.1.4. Risk control

Risk control refers to the ongoing review and monitoring of the risk factors, the risk management as well as the risk responses. These should be adjusted or improved if necessary (Kosub, 2015). As risks change, the risk management and the risk responses have to change too. Thus, the company continuously needs to monitor operations, in order to control and adjust procedures to maintain the best possible risk responses (Waters, 2011).

2.4.1.5. Risk culture and risk government

Since a big part of cyber incidents occur due to different actions of people and user faults, implementing a rich risk culture at the company is very important, in order to reach a holistic cyber risk management. This can be done through training of all employees and regularly testing of IT systems, for instance (Kosub, 2015). Khojasteh (2018) further proposes the company to invest in personnel specifically in charge of the company’s risk management.

2.4.1.6 To summarize

Kosub (2015) stresses the fact that in order to create an efficient cyber risk management, the company needs to continuously evaluate, assess as well as control possible risks. This is agreed upon by Refsdal et al. (2015), who mention one process for monitoring and reviewing of different cyber risks and one process for monitoring and reviewing of the company’s risk management in terms of cybersecurity. Kosub (2015) further mentions a more holistic cyber risk management to be important, which the entire company (suppliers, employees etc) is part of. Adequate IT security, cyber insurance and appropriate risk responses are three very vital parts of an effective cyber risk management too.

It might be understood as Kosub (2015) focuses on a more holistic view of the cyber risk management process, where said author addresses pre and post work (i.e. finding the context (pre) and monitoring the findings (post)). Above mentioned author proposes strengthened work with employees as well as the entire company, in order to achieve a more holistic environment. In comparison, one might say that Refsdal et al. (2015) “attack” the risks more,
where emphasis is put on finding, evaluating and making sure the right risks and responses are found. Both of the cyber risk management processes could be considered good and thoroughly worked through, but a combination of the two might be seen as more beneficial. In that way, a more holistic view is achieved as well as the risks are accessed in a deeper way. Right now, one could perhaps say that Refsdal et al. (2015) process is one small, more focused part of Kosub (2015) bigger and more holistic process. The two processes can be seen in pictures below.

Picture 1: Kosub’s (2015) cyber risk management process (made by the author of this thesis)  
Picture 2: Process for cyber risk assessment (Refsdal et al., 2015, p. 36)
2.5 Summary of the conceptual framework

Below, a table summarizing the conceptual framework can be found.

Table 1: Summary of the conceptual framework

<table>
<thead>
<tr>
<th>Conceptual concept</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk management</td>
<td><em>Risk management</em> is described by Refsdal et al. (2015) as a process, which “…comprises coordinated activities to direct and control an organisation with regard to risk.” (p. 12). Waters (2011) instead describes risk management as a process, where the organisation systematically identify, analyse and respond to risk. Since all organisations are somehow exposed to risks, managing of risk is very important.</td>
</tr>
<tr>
<td>Cyber risk management</td>
<td><em>Cyber risk management</em> is one type of risk management, closely related to risk management in general, and can be described as the management of cyber risks, where the risks are caused by a cyber threat (Refsdal et al., 2015; Kosub, 2015; Griffor, 2017). Lack of knowledge: What type of cyber risk management is performed at online fashion companies in Sweden? Answers will hopefully be gained from the interviews.</td>
</tr>
<tr>
<td>Cyber threats</td>
<td>Refsdal et al. (2015) describe two different types of <em>cyber threats</em>: malicious and non-malicious. Malicious cyber threats are internal, while non-malicious cyber threats are external. Malicious threats could, for instance, be denial of service (DoS-threats), where intentional attacks are made. Non-malicious threats could be crashing systems due to programming errors, for example, or loss of Internet connection due to faulty cables or hardware failure. According to MacDonnell (2014), cyber attacks are one type of cyber threats.</td>
</tr>
</tbody>
</table>
threat, which often is an act of organised crime. Cyber attacks can furthermore be divided up into espionage or sabotage, where espionage refers to illegal information retrieval and sabotage is described as intentional damage to IT-systems (Kosub, 2015).

Lack of knowledge: Which cyber threats are most common at Swedish online fashion companies and what is done to prevent as well as respond to these? Answers will hopefully be gained from the interviews.

**Cybersecurity**

*Cybersecurity* refers to the security of a system, in order to avoid a cyber threat (Refsdal et al, 2015). Kosub (2015) instead describes cybersecurity as protecting any electronic information, the communication technology it depends on and the cyberspace-users.

Lack of knowledge: Do Swedish online fashion companies prioritise cybersecurity? To what extent? Answers to this will hopefully be gained from the interviews.

**The cyber risk management process**

Lack of knowledge: How are cyber risk management processes performed in Swedish online fashion companies? Is it different from company to company? Answers to this will hopefully be gained from the interviews.

| 1. Risk identification | In order to manage the risks, these have to be identified. Thus, identification of cyber threats, which can turn into risks, is needed (Kosub, 2015). According to Waters (2011), risk identification is a process, which helps to review uncertainties in a supply chain and list the most significant associated risks. Both Kosub (2015) and Refsdal et al. (2015) further stress the importance of identifying valuable firm assets, which are vital for the company. |
| 2. Risk assessment and valuation | There is a need to estimate possible losses as well as the likelihood of the identified cyber risks happening (Kosub, 2015), which is done through analysing and assessing of cyber risks. Waters (2011) and Refsdal et al. (2015) mean that it is important to estimate how likely it is for the identified cyber threats to occur, the consequences brought and how difficult it would be for the attackers to reach company assets. |
| 3. Risk response | After having identified the risks and calculated for their likelihood of happening, the best responses to the risks need to be selected and implemented. The best response usually depends on the significance of the risk, i.e. its potential impact (Waters, 2011). There are different ways of responding to risks, where Kosub (2015) identifies four different types that can be applied: risk avoidance, risk mitigation, risk transfer or risk acceptance. |
| 4. Risk control | Risk control refers to the ongoing review and monitoring of the risk factors, the risk management and the risk responses, as |
these should be adjusted or improved if necessary (Kosub, 2015).

| 5. Risk culture and risk government | Since a big part of cyber incidents occur due to different actions of people, implementing a rich risk culture at the company is very important, in order to reach a holistic cyber risk management. This can be done through training of employees, for instance (Kosub, 2015). |
3. Methodology chapter

In the upcoming chapter, the chosen methodology for this thesis will be described. A qualitative exploratory research method in terms of semi-structured interviews is chosen. In order to gain detailed knowledge about Swedish online fashion companies’ current cyber risk management and cybersecurity, semi-structured face-to-face as well as phone interviews seemed appropriate. In order to understand what companies should consider in the field of cybersecurity, experts Magnus Lindegren and Ulf Gustafsson were interviewed over the phone. An operationalization with the connection between the interview questions and the theory, will help the reader to understand the purpose even better. In the end, a summary of the methodology chapter can be found.

3.1 Research strategy: Qualitative research

The choice of methodology and research strategy should be motivated by the purpose of the study (Carlsson, 1991; Bryman & Bell, 2015). In order to best answer the purpose of investigating how cybersecurity risks are managed in Swedish online fashion companies, the chosen research strategy will be a qualitative one. This method generates rich and deep data gained from just a few respondents, and could be beneficial in unfolding various organizational processes (Carlsson, 1991; Gerring, 2007; Doz, 2011). Doz (2011) further explains contributions from different sources to enhance the qualitative research, which thus provides a greater completion in the phenomenon being researched.

One type of qualitative research is exploratory research, which is implemented when the author’s knowledge about a specific topic, subject or question is scarce or when a problem needs more precise definition (Jacobsen, 2002; Flynn & Foster, 2009; Stevens & Wrenn, 2013). Since there is limited availability of previous studies in the field of cybersecurity amongst Swedish online fashion companies and hence, a gap in the literature, an exploratory qualitative approach appeared to be the most suitable. The aim of reaching a better understanding of the subject is also supported by the choice of research method. Furthermore, a qualitative research strategy can help collect data through, for instance, observations, interviews or focus groups (Flynn & Foster, 2009). For this specific study, interviews are chosen and will be explained in detail below.
When explaining the relationship between theory and research, *deductive* and *inductive reasonings* are mentioned. Qualitative research is most commonly seen as a deductive reasoning, where this method often is used when trying to apply a general concept to a specific event (Flynn & Foster, 2009; Bryman & Bell, 2011), which is the case for this study. Cybersecurity in general has been fairly well researched during the latter years, but knowledge about cybersecurity in online fashion companies, more specifically Swedish online fashion companies, is more scarce. Thus, a qualitative research with a deductive approach, which generates findings based on theory (Carlsson, 1991; Bryman & Bell, 2015), seemed like the most appropriate choice.

### 3.1.1 Criticism towards the chosen research strategy

Bryman and Bell (2011) mean that a qualitative research provides understanding of respondents’ behavior. If the fashion companies’ behavior could be based on the respondents’ answers, i.e. the respondents would be the representation of the companies, one could say that this study looks into the respondents’ behavior. Furthermore, Carlsson (1991) together with Bryman and Bell (2015) describe qualitative research to be difficult to generalize. For this study, three Swedish online fashion companies might not be a sufficient number of respondents for the researcher to be able to generalize the information into a bigger picture. However, understanding these companies’ current cyber risk management and cybersecurity still could provide both other online companies and future research with important information. In addition to this, the expertise of the two cybersecurity experts shed an important and general light to the phenomena in order to easier generalize the information onto other companies and businesses.

Furthermore, Carlsson (1991) and Bryman and Bell (2011) explain qualitative research to easily become too subjective, where the researcher interprets the data in a biased way. In line with this, each interview and the results from this interview will be compiled into a follow-up email to be approved by respectively respondent, in order to lower the bias of interpretation of the results. This enhances the study in terms of trustworthiness, where the information is assured and approved to be published by each of the respondents.
In qualitative research, the term “saturation” tends to be brought up. Saturation could be explained as the same answers occurring over and over during the data collection and thus, no more new information is to be found (Bryman & Bell, 2011). When this is the case, the researcher understands that no more collection of data is needed. As saturation has become the marker for sampling adequacy (O’reilly & Parker, 2013), it might be argued that information gotten from three Swedish online fashion companies and two cybersecurity experts might not be sufficient. However, Denzin and Lincoln (2005) firmly explain that there is no “perfect way” to ensure the quality of qualitative research, as it is so diverse. Originally, the notion of saturation was related to grounded theory, but is nowadays applied to all types of qualitative approaches. Since there are so many different types of qualitative approaches, O’reilly and Parker (2013) mean that each approach should be evaluated against different quality markers. Thus, saturation becomes a faulty marker to decide sample size adequacy in every form of qualitative research. Instead, Yin (2009) means that quality of qualitative research rather relates to sampling adequacy providing depth and maximal opportunity for transferability of the findings. Furthermore, O’reilly and Parker (2013) explain that in qualitative research, it is important to explore a range of experiences as well as different opinions and representations of a specific topic. In line with this, Bauer and Gaskell (2000) mean that the number of required participants for a qualitative study heavily depends on the topic and the resources available. For this specific study, opinions have been gathered from three different online fashion companies as well as two cybersecurity experts in order to explore a range of opinions. Additionally, several online fashion companies were contacted prior to this study, whereof only three of these were prepared to help with the data collection. Finally, O’reilly and Parker (2013) mean that the sample size should be correlative to sufficiently answering the study’s research questions, and thus should consist of participants who are most suitable for the research topic.

As this qualitative study brings on a deductive approach, the information scope will be much broader than one with an inductive approach, as the researcher cannot foresee what types of categories will emerge from the data collection. With this in mind, O’reilly and Parker (2013) mean that achieving saturation through a deductive approach, becomes an unrealistic goal.
3.2 Research design: a case study

The research design can be seen as the framework and the structure used when collecting and analysing data (Bryman & Bell, 2011). For the purpose of this paper, a case study seemed like the most appropriate research design, as this type of design helps the researcher to gain detailed knowledge about a specific case as well as it provides explanations (Gerring, 2007; Green, 2007; Flynn & Foster, 2009). Furthermore, a case study research design is strongly linked to qualitative research (Gerring, 2007), where the deductive reasoning of applying general knowledge onto a single case is implemented. For this paper, the “case” could be referred to as the management of cybersecurity in Swedish online fashion companies. This would, in theory, also make the study easier to generalize, since more than one specific company is studied (Bryman & Bell, 2011). According to Baxter and Jack (2008), finding a variety of data sources to approach the case, allows for different angles of the phenomena to be understood. For this study, this is done through interviewing different knowledgeable people from different companies. Green (2007) further explains a case study to be of help when investigating a specific problem in order to reach a solution, which could lead to modifications and improvements of a specific setting. This is in line with the purpose of this paper; in order to investigate how cybersecurity is managed in Swedish online fashion companies and what could perhaps be done if cybersecurity is not yet prioritised, in order to attain a higher level of organisational cybersecurity. Furthermore, both Hyde (2000) as well as Baxter and Jack (2008) mean that a case study can answer qualitative questions like how and why, which is applicable to this study’s second research question of how Swedish online fashion companies handle cyber risks. Additionally, a case study provides several opportunities for testing theory, according to Green (2007). This is in line with the overall deductive approach of this study, where current theory about cybersecurity is tested during the interviews.

There are different types of case studies, according to both Green (2007) as well as Mills, Durepos and Wiebe (2010), where intrinsic, instrumental and collective case studies are mentioned. Baxter and Jack (2008) together with Mills et al. (2010) further mean that it is often difficult to categorize a case study, as the different approaches are very similar, whereas intrinsic and instrumental case studies are the ones closest related. The difference between intrinsic and instrumental case studies is not the case itself but the purpose of the study. An
intrinsic case study is often more exploratory in nature and the researcher is interested in the case more than being able to understand a phenomena and generalize the findings. An instrumental case study is instead helpful when understanding a particular phenomenon better as well as providing insight into an issue, whereas the case becomes secondary. Additionally, in an instrumental case study, the focus of the study is known in advance and thus designed around already established theory. Hence, an instrumental case study focuses on understanding one case, for example a specific research question, a management problem or a particular issue, in order to redraw generalizations into a broader perspective to identify themes to be compared with other cases. For this specific study, both an intrinsic and an instrumental case study could be applicable. As the study is exploratory with a great focus on the case of cybersecurity in Swedish online fashion companies, an intrinsic case study could be suitable. On the other hand, it would also be preferable to understand the phenomenon of cybersecurity in Swedish online fashion companies in a way to generalize the findings easier. However, as the focus of this study is known in advance and designed around already existing theory, the instrumental case study seems like the most appropriate choice of research design.

In the instrumental case study, the sampling of respondents is very crucial in order for the case to yield the right data in connection to the research questions (Mills et al., 2010). For this specific study, importance lies in interviewing the right candidates in order to gain sufficient information to answer the purpose and the research questions.

3.2.1 Criticism towards the chosen research design
Green (2007) recognizes some drawbacks of case studies. In general, results from case studies are not scientific generalizable and the researcher’s bias might interfere with validity of findings. This is underlined by Gerring (2007) too, who means that the respondents examined in a case study often are not considered a perfect representation of the population. Bryman and Bell (2011) stress this as well, and prompt that research from case studies cannot be generalized at all. However, since the researcher of this paper decided to conduct an instrumental case study, it would, in theory, be easier to generalize the findings, even though Mills et al. (2010) present it as an “extension of experience” rather than generalization. Furthermore, a case study research design is also seen to be time consuming and most often
generates in more data than can actually be analysed (Green, 2007). For this study, the method of analysis will be based on theory and then applied to the findings. This could, in turn, make the focus of the analysis more clear. The method of data analysis will be closer described further below.

3.3 Data collection method: semi-structured interviews

Turner (2010) explains interviews to provide great in-depth information about the interviewee’s experiences and point of view on a specific topic, where various forms of interviews can be used in order to receive thick and rich data. According to Bryman and Bell (2011), the researcher can choose between three different types of qualitative interviews; structured interviews, unstructured interviews as well as semi-structured interviews. For this specific study, the chosen data collection method is semi-structured interviews. The main reason for this is the advantage of the researcher having a general base of questions with a clear focus on what to research, even though the order of the questions is allowed to be changed as the interview progresses, which is described by Bryman and Bell (2015). Additionally, semi-structured interviews are considered a good choice when the researcher only has one possibility to talk to the interviewee (Boyce & Neale, 2006), which is the case for all of the interviews in this study. Interviews are furthermore considered flexible and can be conducted face to face or over the phone (Jacobsen, 2002; Gillham, 2005), where phone interviews are suitable when there is limited possibility to physically meet the respondent (Gillham, 2005). However, it is important to schedule the phone interview when it is convenient for the interviewee, in order for him/her to feel comfortable enough to give as accurate responses as possible (Burke & Miller, 2001). After an interview, it is suggested to compile a smaller follow-up letter sent by email, for instance, in order to explain to the interviewee what was uncovered during the interview (Gillham, 2005).

In total, five interviews were conducted with three different Swedish online fashion companies and two cybersecurity experts. Company 1 is a smaller fashion company operating in 13 different markets, with a focus on Scandinavia and the Nordic countries. Company 2 is also a smaller fashion company operating in 30 countries, with more than 2000 employees. Lastly, Company 3 too is a smaller fashion company, currently operating in 35 countries world-wide. The interviews performed with the three Swedish founded and based fashion
companies were very helpful in order to gain detailed knowledge about their current cybersecurity and cyber risk management. This knowledge will furthermore provide help when understanding where there is a lack of knowledge in the field of cybersecurity amongst [Swedish] online fashion companies.

The two cybersecurity experts interviewed were Swedish police superintendent and head of frauds Magnus Lindegren and co-partner of PrimeSafe Ulf Gustafsson. Since 2004, Swedish company PrimeSafe has been assisting companies in all kinds of security issues and managing of risks (PrimeSafe, 2018). In order to understand what online companies should consider when it comes to cybersecurity, Magnus Lindegren and Ulf Gustafsson provided their expert opinion. Merging this information together with Swedish online fashion companies’ current position in cybersecurity, could provide an idea of how cybersecurity better could be managed in [Swedish] online fashion companies. Additionally, these two aspects of the field of cybersecurity, will together create a more holistic view of the subject.

3.3.1 Criticism towards the chosen data collection method

The most prominent disadvantage of interviews is the aspect of time; interviews are seen to be very time consuming (Boyce & Neale, 2006). Another obvious drawback of interviews could be the questions. For instance, the researcher must make sure to not collect irrelevant data through unnecessary questioning (Gillham, 2005; Turner, 2010; Beyers et al., 2014). For the purpose of this study, the interview questions are based on the conceptual framework, in order to make sure the questions would generate relevant information. Additionally, when conducting face to face interviews, it is common for the respondent to avoid answering intimate questions, if the interviewer is seen as a stranger (Carlsson, 1991; Jacobsen, 2002). Face to face interviews might, on the other hand, result in more honest answers (Bryman & Bell, 2011). Researchers (Burke & Miller, 2001; Jacobsen, 2002; Gillham, 2005) also stress the importance of the interviewer to not impact the interviewee’s answers in any way.

In reference to phone interviews, one drawback could be the recording. Burke and Miller (2001) mean that phone interviews might require specific equipment. If the interviewer would like to record the interview, it is further proposed that the recording method should be tested several times prior to the actual interview, in order to avoid issues like mishearing the
interviewee or non-working equipment. Gillham (2005) and Irvine (2010) further stress research to claim phone interviews to result in loss of meaning, due to lack of visual body language. A solution to this could be to conduct the interview over Skype or similar computer programs.

3.4 Interview guide

An interview guide is helpful when conducting unstructured or semi-structured interviews. In reference to semi-structured interviews, an interview guide is supposed to contain issues or questions to be addressed during the interview (Bryman & Bell, 2011). Boyce and Neale (2006) differentiate between an interview guide and an interview protocol, where the interview guide is described as a list of questions or issues to explore during the interview, while an interview protocol is described as the instructions for the interviewer to follow for every interview, in order to ensure consistency in all interviews. This, in turn, increases reliability of the findings. The author of this paper decided to put the interview guide and the interview protocol together, which can be found in Appendix 1 and 2. Turner (2010) underlines a couple of important aspects to cover before the interview starts. For instance, it is important to explain the purpose of the study and the interview, describe how long the interview will take as well as ask the interviewee if there are any additional questions after the interview. All of these aspects are also covered in Appendix 1 and 2, where Appendix 1 refers to the interview guide for the online fashion companies and Appendix 2 refers to the interview guide for the cybersecurity experts.

In a semi-structured interview guide, a certain order of interview questions can be found, but the interviewer needs to be flexible enough to change the order of the questions during the actual interview, if needed (Bryman & Bell, 2011). It is important that there are no more than 15 main questions, that the questions are open-ended and not leading (Boyce & Neale, 2006). Follow-up questions are also considered an important part of the semi-structured interview, in order for the interviewer to obtain optimal responses from the interviewee (Turner, 2010). Carlsson (1991) and Merriam (2009) mean that there are no rules referring to the order of the questions, but suggest that the interviewer starts with neutral questions and end with more sensitive questions, such as age or sexual orientation. Bryman and Bell (2011) instead explain it to be preferable to start with the more sensitive questions, such as name, age and position at
the company, in order to get to know the interviewee better. For this thesis’ interviews, it felt more natural to begin with the more sensitive questions, in order for the author to get to know the interviewee better. However, if anonymity was desired by the interviewee, question one was consequently removed.

Before conducting the actual interviews, it is suggested by Turner (2010) to conduct a pilot interview, in order to try out the questions and see if the order of the questions is suitable and creates a good flow for the interview. Unfortunately, there was no pilot interview conducted for this thesis, since there was no possibility for more than one actual interview with each of the suitable respondents. However, the interview questions were looked through by the supervisor Jonas Larsson, who gave a few comments in order to improve them. As mentioned before, to finalize each interview, a follow-up email with a summary of what was said during the interview, will be compiled. This summary should be approved by the interviewee, in order to determine the accuracy of the interview.

3.4.1 How the interviews were conducted

3.4.1.1 Company 1 and Company 2

The interviews were conducted in a quiet room at the headquarters of respectively company, where only the interviewer and the interviewee were present. At Company 1, the CTO was interviewed and at Company 2, the CIO was interviewed. Carlsson (1991) and Turner (2010) mean that it is important to be in a quiet surrounding during the interview, in order to not be disturbed, to make the interviewee feel comfortable and to assure the quality of the recording. In consent, both of the interviews were recorded on the interviewer’s mobile phone and saved for later as well as the interviewer took notes on the computer in order to ease the transcription later on. Clifford et al. (2010) together with Turner (2010) mention the benefit of both recording the interview and taking notes, since it sometimes can be difficult to comprehend everything during the interview as well as remember the answers after the interview. Most often, it is necessary to go back and listen to the interview again. Before the interview, the subject and the purpose of the interview was explained to the respondent. This is important, according to Carlsson (1991) and Burke and Miller (2001), since it prepares the interviewee for the upcoming questions in a better way. Both of the interviews took approximately 40 minutes each, which is a good standard duration of an interview, according
to Jacobsen (2002). As mentioned above, in semi-structured interviews, the interviewer is allowed to change the order of the questions during the interview, even though a certain order of the questions is set (Bryman & Bell, 2011). During the two interviews, the order of the questions changed differently as well as follow-up questions were created along the way. However, a variation of follow-up questions came to mind during the two interviews.

Both of the interviews were conducted in Swedish, since the respondents and the interviewer are of Swedish nationality, and the interviews were then translated into English. Squires (2008) mentions the drawbacks of this procedure, since the translation of the answers could easily turn out biased, but still do not propose a professional translator to be the solution. Furthermore, both Carlsson (1991) and Bryman and Bell (2011) mean that when there is only one researcher in charge of every part of the interview process (i.e. writing the interviews, conducting the interviews as well as compiling the interviews), it is not necessary to get professional help and the process can thus be performed by the researcher herself. In the next section, 4. Results, the information gained from the interviews with the Swedish online fashion companies, can be found.

Since there was only one possibility to meet with the CTO respectively the CIO, a follow-up conversation with a summary of what was said during the interview was compiled. This summary was approved by the interviewees, in order to determine the accuracy of the interview and to assure the interviewees of what information will be published. This procedure is proposed and highlighted by Gillham (2005).

3.4.1.2 Company 3

The interview with Company 3 was conducted via a Facebook phone call, as a phone interview is a possible solution when there is a geographical distance (Gillham, 2005). The interview was scheduled beforehand through email and took place in a quiet surrounding. Since the interview was conducted through the computer, there was possibility to record the interview through the interviewers mobile phone. Thus, in consent with the interviewee, the interview was recorded and saved for later. Clifford et al. (2010) and Turner (2010) propose the interviewer to always record the interview, to make the following transcription easier. In addition to this, notes were also taken. Before the interview, the purpose of the thesis was
explained to the interviewee. The same 15 questions, as for the other fashion companies, were asked, but the duration of the phone interview turned out to be approximately 16 minutes. This is, according to Irvine (2010), common; phone interviews often tend to be shorter than face to face interviews. The interview was conducted in Swedish and later on transcribed into English. Since the same person is in charge of the entire interview process, Carlsson (1991) and Bryman and Bell (2011) approve of this. In order to validate the interview as well as the answers, a summary of the interview was send to the respondent for approval. The results from the interview can be found below in chapter 4. Results.

3.4.1.3 Police superintendent and head of frauds Magnus Lindegren and co-partner of PrimeSafe Ulf Gustafsson

The two interviews with the cybersecurity experts were conducted over the phone, one by one, due to geographical limitations. The phone interviews were previously scheduled through an email conversation between the interviewee and the interviewer. As a primary data collection method, phone interviews are common in qualitative research and often conducted when there are difficulties to meet the respondent in person (Burke & Miller, 2001; Irvine, 2010). Interviewing experts means interviewing a person with substantial knowledge in a specific field, which needs to be taken into consideration. Asking the right questions in a professional manner, could generate in a lot of meaningful information (Beyers et al., 2014).

Before the interview, the subject and the purpose of the study was explained in order to prepare the interviewee. The interviews took place in a quiet surrounding and had a duration of approximately 30 minutes each. Both of the interviews were conducted in Swedish, since the interviewees and the interviewer are of Swedish nationality. Only one follow-up question came to mind during the interviews, and the questions were asked in the written order, which also is acceptable according to Bryman and Bell (2011). It was not possible to record the phone interviews, which is a common problem according to Burke and Miller (2001), since most researchers do not have the required equipment. However, for this study, the interviewer took complete notes on the computer during the interviews. Hence, the pause in-between questions was a bit longer. A summary of each interview was compiled and send by email to respectively respondent afterwards, in order for them to approve. This would further help
determine the accuracy of the interview and assure the interviewees of what information will be published. In the next section, 4. Results, the information gained from the cybersecurity experts can be found.

### 3.5 Operationalization for the online fashion companies

The table below reveals the connection between the interview questions and the conceptual framework.

**Table 2: Interview questions for the online fashion companies and the thought behind them**

<table>
<thead>
<tr>
<th>Interview questions</th>
<th>Conceptual framework</th>
<th>Information desired</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. What is your name and what is your job position?</td>
<td>-</td>
<td>Personal information about the interviewee. Q1 will be removed if anonymity is desired by the respondent.</td>
</tr>
<tr>
<td>2. What are your main work tasks?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. For how long have you been working here?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Have you had similar jobs before? In that case, did you have similar/the same work tasks?</td>
<td>Cybersecurity</td>
<td>To understand if/how cybersecurity has been prioritised and managed in companies during the latter years.</td>
</tr>
<tr>
<td>5. What kind of risk management is performed at the company? How involved are you?</td>
<td>Risk management</td>
<td>Getting to know more about the company’s risk management in general.</td>
</tr>
<tr>
<td>6. To what degree is cybersecurity prioritised at the company?</td>
<td>Cybersecurity</td>
<td>Understanding the company’s current posture towards cybersecurity.</td>
</tr>
<tr>
<td>7. How do you assess the company’s cyber risks? Is the company very, fairly or not at all exposed to cyber risks?</td>
<td>The cyber risk management process; cyber risks and cyber threats</td>
<td>Gaining knowledge about the company’s cyber risk management process and its different parts.</td>
</tr>
<tr>
<td>8. What kind of cyber risks are the most common for the company? What is the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td>Response</td>
<td>Additional Information</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>likelihood of these happening?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. How does the company respond to cyber risks and threats, if they would occur?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Could you please walk me through the company’s cyber risk process.</td>
<td>The cyber risk management process</td>
<td>Getting a clearer picture of the process.</td>
</tr>
<tr>
<td>establishing of cybersecurity to treatment of cyber threats.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Has the company had any exposure to cyber threats recently? If yes, what happened and what was done?</td>
<td>Cyber threats; the cyber risk management process and treatment of cyber threats</td>
<td>Gaining information about an eventual, specific case and the cyber risk management process implemented and connected to this.</td>
</tr>
<tr>
<td>12. Does the company have specific personnel in charge of risk management, specifically cyber risk management? If yes, what is this personnel’s main tasks?</td>
<td>The cyber risk management process</td>
<td>Understanding the company’s risk management position and the personnel’s part in avoidance of exposing the company to (unnecessary) risks.</td>
</tr>
<tr>
<td>13. To what degree is the rest of the company’s staff educated and knowledgeable in risk management, cyber risk management and all of the accompanied parts of the processes?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14. To what degree is the company’s staff educated in what they themselves can do when it comes to avoiding cyber risks?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15. Is there anything you would like to add?</td>
<td>-</td>
<td>To find additional, perhaps overlooked, information</td>
</tr>
</tbody>
</table>
3.6 Operationalization for the cybersecurity experts

The table below reveals the connection between the interview questions and the conceptual framework.

Table 3: Interview questions for cybersecurity experts and the thought behind them

<table>
<thead>
<tr>
<th>Interview questions</th>
<th>Conceptual framework</th>
<th>Information desired</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Please state your name and current work position. 2. What are your main work</td>
<td>-</td>
<td>Personal information about the interviewee.</td>
</tr>
<tr>
<td>tasks?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. When did your interest for cybersecurity and cyber risk management emerge?</td>
<td>Cyber risk management; cybersecurity</td>
<td>To understand when cybersecurity became important and which companies actually prioritise this.</td>
</tr>
<tr>
<td>4. What kind of companies do you encounter in your daily work?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. To what degree would you say cybersecurity is prioritised amongst companies today?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Where do companies lack knowledge? What should be considered? 7. What are your</td>
<td>Cyber risk management; cybersecurity</td>
<td>To perhaps find weaknesses in companies’ current cyber risk management.</td>
</tr>
<tr>
<td>expert tips to companies operating online?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Is there anything you would like to add?</td>
<td>-</td>
<td>To find additional, perhaps overlooked, information.</td>
</tr>
</tbody>
</table>

3.7 Method of data analysis: qualitative content analysis

The final part of the interview process is to analyse the data gathered from the interviews, in order for the researcher to understand what was uncovered during the interview and to compile the data (Turner, 2010). One very important part of this is to distinguish between relevant and irrelevant data, according to Gläser and Laudel (2013), in order to reduce the data to only work with and present data necessary to answer the purpose of the study. Not
everything said during the interviews is helpful when answering the research questions. When only the relevant data is picked out, it is time to compile and make sense of the information. The qualitative data is often compiled into sections or groups called themes, which could be expressions, ideas or common phrases amongst the interviewees (Flynn & Foster, 2009; Turner, 2010). This is underlined by Boyce and Neale (2006) too, who suggest the researcher to read through the interview and look for patterns or themes, which could be found in the interviewees’ answers. If there is a variety of themes, it is proposed to group the themes in a meaningful way. In this phase, according to Baxter and Jack (2008), it is important to remember the holistic view of the gathered data, and not report the findings separately but instead in a way for the reader to understand the overall case. As concerning this study, it is important to decide in what language the data analysis should be performed, before the actual analysis takes place (Squires, 2008). In this case, the gathered data was translated from Swedish to English before the analysis took place.

Finding themes and patterns amongst the answers, also referred to as qualitative content analysis (Turner, 2010; Gläser & Laudel, 2013), will be the method of data analysis for this study. Since there was a great amount of information obtained from all of the interviews, a crucial part will be to select the most relevant data to then group into themes. According to Gläser and Laudel (2013), there are different ways of conducting qualitative content analysis; either the categories are derived from theory and then applied to the data, which is considered deductive, or the categories are derived exclusively from the data, which is considered inductive. For this paper, categories will be derived from the conceptual framework, specifically The cyber risk management process, which then will work as “headlines” for the gathered empirical data to be compiled under. This is furthermore in line with the overall deductive approach of the study.

3.8 Ethical issues
When conducting research, the aspect of ethical issues is constantly apparent, where confidentiality and anonymity are included (Carlsson, 1991; Bryman & Bell, 2015). For instance, all interviewees might not be comfortable with having information about them published (Flynn & Foster, 2009). In that case, Carlsson (1991) means that anonymity could be the solution. Additionally, it is important to also change the name, location and description
of the company if the interviewee desires anonymity. Prior to the interview, a written or documented oral consent is necessary to get from the interviewee (Carlsson, 1991; Boyce & Neale, 2006). As a part of the consent, the interviewee should be informed if any recording equipment will be used during the interview (Bryman & Bell, 2011).

For this specific study, an oral consent was gotten from each of the interviewees before the interview took place. The interviewees were also informed of the possible recording of the interview, the purpose of the study and how the obtained information will be used further. After the interview, a follow-up conversation with a summary of what was said during each interview was emailed to respectively respondent. At this stage, the interviewee was also asked if anonymity was desired for the paper, i.e. if the name and workplace were not to be revealed. Two out of three online fashion companies desired anonymity, in order to not expose respectively company to unnecessary risk. A decision was thus made to anonymize the answers from all three companies and the first interview question was thereby removed. Furthermore, in chapter 4, where the results from the interviews will be revealed, the companies will continued to be named Company 1 (C1), Company 2 (C2) and Company 3 (C3), without any type of ranking. The cybersecurity experts Ulf Gustafsson and Magnus Lindegren approved of having their name and work position revealed.

3.9 Sampling
Carlsson (1991) and Turner (2010) stress the importance of selecting the right candidates for the interviews, who will provide the most accurate and valid information. For the purpose of this study, a non-probability sample was implemented, since the respondents were non-randomly selected (Flynn & Foster, 2009; Dane, 2011). In reference to the online fashion companies, it was important to select people representing these, in order to get as accurate information as possible. The selected respondents further had to have some kind of involvement in the company’s IT solutions or website. This was important both for them, in order to be able to understand and answer the questions accurately as well as for the study, in order for the right information to be obtained. This type of sampling is described by Turner (2010) as criterion based sampling, which is used to obtain the most qualified candidates, who would provide the most credible information. For the purpose of this study, it was important to interview Swedish fashion companies, who partly or entirely operate their
business online, in order to get as accurate answers as possible. Answers about risk management in connection to physical stores were not of interest.

When selecting Swedish police superintendent and head of frauds Magnus Lindegren and CEO of PrimeSafe Ulf Gustafsson as samples, a *convenience sample* was conducted. This is described by Bryman and Bell (2011) as an easily available and accessible sample for the researcher. Paths crossed with Magnus Lindegren and Ulf Gustafsson at a lecture about cybersecurity at Ellos in Viared, Borås, previously this spring. In this context, both are considered experts in the field of cyber risk management, and thus were chosen to give dynamics to the study and a different view of the management of cyber risks.

### 3.10 Quality criteria
For qualitative research, Bryman and Bell (2011) mention trustworthiness and authenticity. Trustworthiness can be referred to as if the results of a study allows for repetition, and authenticity could be a measurement used to determine if the researcher is measuring what is stated or not. Gerring (2007) further explains internal and external validity as important parts of validating the results of a case study. Internal validity refers to the validity of the respondents and their answers, and external validity refers to the generalizability to a broader population. Both Gerring (2007) and Bryman and Bell (2011) highlight the difficulties of generalizing findings from only a small number of respondents in a case study. However, for this study, an instrumental case study of one case with several respondents, i.e. the three online fashion companies, is conducted, which would allow for generalizability in an easier way (Green, 2007). Additionally, Gerring (2007) means that for a case study, the internal validity is seen as the most important aspect, and thus, it is more important to be able to assure the validity of the respondents’ answers than to generalize the results.

For this study, all of the planned and executed steps in the gathering of empirical data, has carefully been accounted for and thus, repetition would be feasible. In fact, Cleary et al. (2014) stress accurate reporting of all qualitative research methods to be of importance and mention comprehension and transparency to be significantly increased, if all stages of the research are well presented for the reader. However, since the interviews were performed in Swedish and later translated into English, Squires (2009) might argue for lack of
trustworthiness and difficulties for repetition. Though, since only one author was in charge of as well as conducted all the steps in the interview process, trustworthiness could be considered increased (Gillham, 2005). Furthermore, authenticity can be translated into the respondents being able to answer truthfully during the interview, according to Bryman and Bell (2011). For this study, the researcher strongly believe the interviewees answered the questions as truthfully as could, bearing in mind the risk of revealing too much of sensitive company information. Additionally, since the interview protocols were carefully followed prior to every interview, i.e. consistency allowed in all interviews, Boyce and Neale (2006) would argue for increased reliability of findings. According to Yin (2009), reliability of findings also influences the extent of findings being replicated.

3.11 Summary of the methodology chapter

Below, a table summarizing the methodology chapter can be found.

Table 4: Summary of the methodology chapter

<table>
<thead>
<tr>
<th>Conceptual concept</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Research strategy</strong></td>
<td><em>Qualitative research</em> is the chosen research strategy, since this method generates rich and deep data gained from just a few respondents (Carlsson, 1991; Gerring, 2007). One type of qualitative research is <em>exploratory research</em>, which is implemented when the author’s knowledge about a specific topic, subject or question is scarce or when a problem needs more precise definition (Jacobsen, 2002; Flynn &amp; Foster, 2009; Stevens &amp; Wrenn, 2013). Qualitative research is most commonly seen as a <em>deductive reasoning</em>, where this method often is used when trying to apply a general concept to a specific event (Flynn &amp; Foster, 2009; Bryman &amp; Bell, 2011).</td>
</tr>
<tr>
<td><strong>Research design</strong></td>
<td>The chosen research design is an <em>instrumental case study</em>, since this type of research design helps the researcher to gain detailed knowledge about a specific case as well as it provides explanations (Gerring, 2007; Flynn &amp; Foster, 2009). Green</td>
</tr>
</tbody>
</table>
(2007) further explains a case study to be of help when investigating a specific problem in order to reach a solution, which could lead to modifications and improvements of a specific setting.

<p>| <strong>Data collection method</strong> | <em>Semi-structured interviews</em> are chosen as the data collection method for this study, since Turner (2010) explains interviews to provide great in-depth information about the interviewee’s experiences and point of view on a specific topic, in order to receive thick and rich data. Semi-structured interviews is of advantage when the researcher has a general base of questions with a clear focus on what to research, but still has the possibility to change the order of the questions as the interview progresses (Bryman &amp; Bell, 2015). Furthermore, semi-structured interviews are considered a good choice when the researcher only has one possibility to talk to the interviewee (Boyce &amp; Neale, 2006). |
| <strong>Interview guide</strong> | In reference to semi-structured interviews, an <em>interview guide</em> is supposed to contain issues or questions being addressed during the interview (Bryman &amp; Bell, 2011). The complete interview guide, with all accompanied aspects and steps, can be found in Appendix 1 and 2. |
| <strong>Method of data analysis</strong> | <em>Qualitative content analysis</em> can be described as finding themes and patterns amongst the answers (Flynn &amp; Foster, 2009; Turner, 2010). Gläser and Laudel (2013) further mention there are different ways of conducting qualitative content analysis; either the categories are derived from theory and then applied to the data (deductive) or the categories are derived exclusively from the data (inductive). |</p>
<table>
<thead>
<tr>
<th>Ethical issues</th>
<th>It is important to consider confidentiality and anonymity as part of <em>ethical issues</em> when conducting qualitative research and interviews (Carlsson, 1991; Bryman &amp; Bell, 2015).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling</td>
<td>For this study, a <em>non-probability sample</em> was obtained, as the respondents were non-randomly selected (Flynn &amp; Foster, 2009; Dane, 2011). The respondents from the online fashion companies were selected through a <em>criterion based sampling</em>, where the most qualified candidates with the most credible information are used (Turner, 2010). When choosing Swedish police superintendent and head of frauds Magnus Lindegren and CEO of PrimeSafe Ulf Gustafsson as samples, a <em>convenience sample</em> was conducted. This is described by Bryman and Bell (2011) as an easily available sample for the researcher.</td>
</tr>
<tr>
<td>Quality criteria</td>
<td>For qualitative research, Bryman and Bell (2011) mention trustworthiness and authenticity as <em>quality criteria</em>. Trustworthiness can be referred to as if the results of a study allows for repetition, and authenticity could be a measurement used to see if the researcher is measuring what is stated or not. Gerring (2007) further mentions internal and external validity as important parts of validating the results of a case study, where internal validity refers to the validity of the respondents and their answers, and external validity refers to the generalizability to a broader population.</td>
</tr>
</tbody>
</table>
4. Results

In this chapter, a description of the results obtained from the five interviews can be found. The first part represents the results gained from the three online fashion companies, and the second part describes the results gained from the two cybersecurity experts. The results from the online fashion companies will follow the same manner as the theory of The cyber risk management process. Thus, the headings included in the process will be used to categorize the gathered data in a meaningful way. The three online fashion companies will remain anonymous throughout this text.

4.1 Results from the online fashion companies

4.1.1 Company 1

At Company 1, the CTO (chief technical officer) was interviewed. The CTO has worked there for 2.5 years, and is currently in charge of the IT-department, which in turn is responsible for the development of the company’s web solutions. The CTO’s main job tasks concern the overall system operations and management of several systems, where the online web is the largest one. This CTO has not worked in fashion and apparel before; instead, this person has a background in health care, retail and books as well as experience from an B2B industrial e-commerce company. Overall, the CTO has been working in IT and management of IT since 1999.

“Working in retail is a lot of fun! It’s a great industry to work in, since you’re handling products everyone can relate to. Working at [Company 1] is also a lot of fun, because it involves working with clothes and accessories, which more or less everyone has a relationship to.”

1. Risk identification

According to the CTO, Company 1 is exposed to cyber risks on a fairly high level, since the company is and always has been a pure e-commerce company. Thus, cybersecurity has always been an important part of the business. The company is working with a couple of partners, for instance a company who is completely in charge of Company 1’s payment solutions. In that case, this payment company has their own cybersecurity, since they are
taking much higher risks with the monetary transactions. The most common cyber risks that have occurred at Company 1 so far, are different types of trespassing. Trying to impose on certain functions on the website to send advertising through the company’s systems and solutions is one example. Thus, the website needs to be identified as an valuable firm asset, which should be taken into consideration when identifying risks. The majority of the cyber attacks are from China and Russia, and they are implemented more or less only by individuals. The CTO means that this is valuable information for the company to possess, in order to know what to protect against and what actions to take if it would happen again.

2. Risk assessment and valuation

Risk management is implemented in every department of the company, where risk assessment is implemented for every system, one at a time. Parallel to that, Company 1 works with safety at the company in a way that does not concern the systems. Instead, the company works more with policies and awareness among the staff. The CTO means that the company is fairly good at educating the staff in these questions, considering the employee turnover. When accounting for the likelihood of identified cyber risks to happen, the CTO means that it is important to look at what has previously happened in order to better protect against this in the future. In this way, the company would also know what measures, if any at all, should be implemented.

“In one specific Chinese case, we could track the IP address to different university networks in the country. Though, we chose not to proceed with any of these, since we felt like the value creation was not enough for us, to actually “catch” and bring this person to justice.”

Social engineering risks, i.e. risks concerning unauthorized people physically entering the company building, was brought up during the interview, as a possible risk for the company. However, the CTO explains the current risk assessment and likelihood when it comes to social engineering risks to be relatively low and further means that perhaps bigger companies would be targeted firsthand.
3. Risk response
The CTO explains Company 1 to have security of all their systems, which is taken care of by different suppliers. Thus, the immediate incident response to a risk, is managed by the suppliers. The firewalls for the website is one example, and if something were to happen there, it is first and foremost up to the suppliers to take care of it. They get indications of this, react accordingly and then report back to Company 1. Consequently, if the company was to terminate or stop an intrusion on the website, it would be in collaboration with the suppliers, since the suppliers have the ability to track and block specific IP-addresses. When a trespassing is terminated, Company 1 evaluates the intrusion together with the suppliers, in order to know how to act and if specific protections might be needed to avoid a repeated experience. Additionally, the IT-department often implement something called “security incident”, as part of their operational readiness. This is handled by the same people, who work with the online web. The CTO means, that according to industry standard, the level of protection against trespassing on the web is very good.

4. Risk control
As mentioned before, after a trespassing or intrusion on the website, Company 1 always evaluates what happened and what was done, in order to improve for the future. Additionally, the staff is continuously educated in risk management and what they can do in order to avoid risks.

5. Risk culture and risk government
According to the CTO, Company 1 possesses a rich risk culture at the company. This is very important, since the employee turnover is high and new employees continuously need education in risk management. During the interview, the CTO explained a new updated information security policy regarding this, called GDPR (General Data Protection Regulation), which will be implemented in May this year. The policy highlights, for instance, the usage of mobile phones and computers in a way that minimizes the company’s exposure to unnecessary risks. The CTO together with the rest of the IT-department are 100% involved in this. The guidelines in GDPR, which is based on the security standard ISO 27 000, will be available for everyone in the staff to read. This document is created together with
professionals in the area, in order to make sure the staff will be educated correctly. Unfortunately, this same information is not provided for interns or consults, according to the CTO. When consults are visiting the company with their own computers, Company 1 always advises them to connect to the wireless guest network instead of the regular network. The guest network doesn’t contain the same access and no sensitive information.

“[Social engineering] is a big part of GDPR, which we are working on right now. I have to say, we can definitely get better at this, and that is why we put so much effort into it.”

When it comes to testing of IT systems to ensure everything works the way it should, risk assessment is regularly carried out for every system. Additionally, ensuring everyone to have the right access to different systems and that it works correctly, is one type of safety effort implemented at Company 1.

4.1.2 Company 2

At Company 2, the CIO (chief information officer) was interviewed. This CIO has worked at Company 2 since October 2017, and the person’s main task is to make sure that the company’s digital environment meets the requirements from the board of directors. The digital environment consists of one strategical part, where the commercial strategy is mapped out, and one operational part, where the environment has to be accessible, trustworthy and secure. The CIO has had similar jobs before, where the previous job position was as a CISO (Chief Information Security Officer). This person also has previous experience from the textile industry, which is from KappAhl. The CIO would like to be described as an “industry or enterprise product”, based on previous work experience from Volvo, Astrazeneca, Ford and Toyota, amongst others.

“One could say that I’m originated from the really big enterprises, which makes [Company 2] a small company for me to work for. Just before I started here, I worked at Schenker as the head of governors for the European region. I got information from a colleague at Schenker, that [Company 2] needed help, since they were facing an extensive restructuring, something we call a “turn around-case”, where you are supposed to turn the trademark upside down.”
According to the CIO, Company 2 (as well as the rest of the textile industry) is currently facing a great digital challenge, and that is why this person got hired. The company needed someone with previous experience and knowledge. Furthermore, the CIO sadly highlights the fact that cybersecurity still is not taken seriously by online companies, even though the phenomenon started emerging approximately 20 years ago. The CIO means that knowledge in cyber risk management is scarce at companies, and there is no willingness to learn either.

1. Risk identification
According to the CIO, the area of cybersecurity is always present at Company 2, but the prioritisation and visibility have increased since this person was hired. Since Company 2’s online sales represent 17-18% of all sales, and thus, a lot of personal financial information is stored, cybersecurity is an important part of the company. Especially sensitive customer information is seen as an valuable asset to protect. The CIO further means that it is important for Company 2, as well as for every other company, to understand what customer information and where it is handled, in order to realize if something would go wrong. This is something that Company 2 highly prioritises right now. Furthermore, Company 2 estimates an 10-15% increase of online sales within the next few years, and thus, the website could be identified as an valuable firm asset as well.

When identifying risks at Company 2, a central risk management model is run. This is done every year, in order to identify risks and responses to these risks. The model is run in all departments of the company, such as financials, stock and logistics as well as the digital parts of the company. According to the CIO, this model covers both commercial and other types of risks.

“The risk management model] is initiated by the board of directors, then it goes on to the concern group and then it is spread downwards in the company. We also have one specific security department, with one specific chief of security, who is solely working with these questions. Normally, this chief of security works with safety questions concerning the stores, but I work closely to him as well.”
Identifying new and upcoming cyber risks is important for Company 2, in order to be prepared and make the right choices if the company would get targeted. The CIO means that Company 2 is part of different forums, where information from suppliers and safety partners can be obtained. Additionally, everyone working in risk management at Company 2, has an interest in finding information on their own as well. Potential risks are then highlighted and discussed during company meetings.

2. Risk assessment and valuation
As mentioned above, Company 2 implements risk management in all parts of the company. The CIO further describes cybersecurity to be part of everything the company does, both online and in stores. However, the CIO is so far not familiar with any online incidents and describes Company 2 to be “lucky” to not have been targeted. However, the industry recently faced an Intel bug, which Company 2 was quick to discuss at a meeting. The company further decided to not act against it, since the risk of impact seemed to small. In time, Company 2 started noticing other companies being targeted, and thus had to rethink their choice of action.

When investigating how difficult it would be for an attacker to reach sensitive company information, Company 2 performs something called “penetration tests”. This could be explained as continuously testing of their systems, to uncover how far one can go with and without credentials. Additionally, the company continuously tests the guest network as well, to see if visitors could access other networks and systems through this.

3. Risk response
In line with the central risk management model, Company 2 responds to risks according to a pre-decided “incident process”. This process explains in detail what will happen, who is doing what and how to proceed after a risk has occurred. Unfortunately, the CIO could not get into detail of this, with regards to sensitive company information. However, it was further mentioned that it is important to be prepared and know how to act. Knowledge seemed to be important as well, where the CIO stresses the difficulties of responding to an incident if the company does not know what system(s) might have been affected.
“Basically, if you know what the risk is, it is easier to make a choice. [...] I mean, it’s hard to respond to an incident if you don’t know what it has affected.”

The CIO further describes Company 2 to outsource some of the company systems to partner companies, and that these partners somewhat are in control when it comes to responding to possible hacker attacks. Though, it does depend on what the attack looks like, since there are different detectors at Company 2’s platform and website. For instance, the company’s website is incorporated with an underlying mechanism, which would immediately terminate an attempt of changing prices of the products online.

4. Risk control

The CIO mentions Company 2 to constantly review risk factors, current and new, on company meetings and on individual level. Furthermore, the company has accountants in charge of annually taking a closer look at the digital part of the company, through digital audits.

5. Risk culture and risk government

Prior to the CIO’s employment at Company 2, the company put minimum effort into implementing a company risk culture and educating the staff. Today, the company is working with both digital and physical audits as well as educating the staff in questions concerning risk management.

“We are [also] working with physical audits. For example, if you come here into the office and start going through the trash, what can you find?”

The entire staff at Company 2, both at the headquarters and in the stores, are currently being educated in GDPR. The CIO means that it is important for everyone to understand what type of personal customer information is being saved, how it is handled and for how long it will be stored. When it comes to access to different systems, Company 2 has an access-team, who is in charge of providing everyone in the staff with the right access. Thus, access cannot be altered by the staff themselves. The CIO further explains the online systems and the online platform to be accessible by a very limited number of people.
4.1.3 Company 3

At Company 3, the Web editor was interviewed. This Web editor has worked at Company 3 for almost four years now, and describes the role as an Web editor to be very broad.

“Web editor at [Company 3] is a broad role, where I’m in charge of different campaigns, newsletters, updating the website as well as being the head of IT projects.”

The Web editor has previous work experience from the fashion industry, where this person worked as an Web editor at Indiska. Before that, this person was employed as an e-commerce project manager for a smaller agency.

1. Risk identification

The Web editor explains Company 3 to be owned by another large, global fashion company and thus, all of the risk management is performed at this company’s IT department instead. The Web editor further describes Company 3 to be “covered” by the global company, their systems and resources, as this company has people in charge of the risk management, and thus forwards all important information to all of their sub-brands, including Company 3. Sometimes, the personnel at Company 3 gets emails with information regarding possible hacker attacks, and is requested to change their passwords, for instance. The Web editor further describes the personnel at Company 3 to be informed when security updates on their computers has to be made or when risky links flourish around the company. Altogether, the Web editor more or less explains Company 3 to be spared from cyber risks. Cybersecurity is indeed present at the company, but perhaps not as prominent. The Web editor thinks this is a result of the global company owning Company 3, where a lot of knowledgeable people work in this field. The Web editor additionally stresses the fact that not many know that this global company owns Company 3. If more people knew, the Web editor means, the company would probably be exposed to more spam and cyber attacks.

2. Risk assessment and valuation

Since the IT department at the global fashion company assess the risks at Company 3, the Web editor is not familiar with any online incidents that has occured. It is again explained that Company 3 has limited exposure to cyber risks. Additionally, the Web editor describes a
Christmas campaign two years ago, where Company 3 invited their customers to share music, tips and Instagram-pictures they liked and found inspiring. This was accomplished through Wordpress, where the Web editor explains two different functions: Company 3 could either decide to view every post before it was published, or they could trust their consumers and let them publish anything without the company’s approval of the content. These posts could then be seen immediately. The Web editor describes Company 3 as taking a chance and chose the latter alternative. The company did expect some spam, but luckily, nothing was received and the idea worked out great.

“It was definitely because [Company 3] isn’t that big of a company. I mean, we are owned by [the global company], but I don’t think people actually know that. If more people knew this, I absolutely think we would have gotten more spam and mean words.”

3. Risk response

Preventively, the global fashion company owning Company 3, has blocked certain web pages and links, due to them being considered risky, the Web editor explains. Unfortunately, this person could not explain any risk responses further. However, the Web editor mentions a team at this global company, who works with risk responses and ensured that they would do everything they could if a threat would occur.

4. Risk control

Since the global fashion company is completely in charge of Company 3’s cyber risk management, it is difficult for the Web editor to know how the monitoring of different risk factors looks like. The global company always provides Company 3 with all the necessary information. Thus, since the company always is informed of possible hacker attacks for instance, they would probably also be notified about new risks and new responses, both on Company 3’s respectively the global company’s level.

5. Risk culture and risk government

As a result of the global company’s involvement in Company 3’s cyber risk management, the Web editor explains Company 3 to not have personnel in charge of these questions. However, the person does explain everyone being employed at the company to complete a couple of
online courses regarding risk management, both in general as well as cyber risk in particular. In these courses, the Web editor imagines preventive measures in terms of cybersecurity to be brought up.

4.2 Results from experts Ulf Gustafsson and Magnus Lindegren

4.2.1 Ulf Gustafsson, PrimeSafe

Ulf Gustafsson is a co-partner for PrimeSafe, which is a company who works with all types of security matters, through finding valuable company information in need of protection. Ulf presents both the company and its current clients as “incident driven”; companies contact PrimeSafe when something has already happened, and thus, PrimeSafe becomes reactive in their work. Ideally, they would like to work more proactively and help companies before an issue has occurred.

“My main work tasks include sales and marketing of our company. I mainly work with finding new customers, and not so much with the investigation of different incidents. I spend my time finding companies with different risks and vulnerabilities, who needs to extend their risk management.”

Ulf interest in security started in the end of the 90s, when IT was growing strong. He quickly understood that it would get easier for criminals and criminality to spread in new and different ways through the help of IT. His thoughts were right, and today, he predicts companies to start hiring new personnel in IT, since it is considered increasingly important. However, he would say that companies still do not understand their risks, which is the biggest part of an effective risk management. Companies do not realize even the most simple risks and problems, and one reason for this is the lack of risk analyses performed at the company.

“Actually, I think this applies to the entire issue of security: companies don’t really know their risks. As a company, what do we have that is worth protecting? What are our assets? That is the biggest flaw, you don’t realize the risks and don’t understand the consequences of these risks.”

PrimeSafe educates companies, board of directors and management teams in the field of risk
management, where cyber risk management is a recurrent subject. In general, companies who lack knowledge in cybersecurity, shows a relatively low prioritisatation of the field. That is what makes them “incident driven”, Ulf means, and thus only contact PrimeSafe when there has already been experienced security problems. Previously, bigger companies with cybersecurity problems were the most common clients for PrimeSafe, but today, smaller companies being targeted by cyber criminals are in need of help too. Ulf describes a small company from Gothenburg, who lost 1 million SEK due to online frauds, which eventually caused them bankruptcy. He means that this is a result of bad risk management routines.

To help companies with their cyber risk management, the most important part is to identify valuable firm assets, according to Ulf. This is done by PrimeSafe, with some help of different partners specialized in cybersecurity. In this case, a “red teaming exercise” is initiated, where a group of professionals hack the company “for fun”, in order to see how easy or difficult it could be. Ulf describes this exercise as giving the “red team” free access to completely penetrate the company, in order to understand what shortcomings there are in the company as well as in the systems.

“The thing is, companies who previously haven’t been exposed to any risks or frauds, or don’t understand that they have been attacked, don’t really care. A lot of big companies, with billions in turnover, don’t even have a head of IT, because they just don’t care! They think they don’t have any problems, and often live by the thought: “if it hasn’t happened, it’s not real”.

Ulf would not consider himself an expert in the field of cybersecurity, but he has gained some important knowledge throughout the years. His top five list of aspects companies need to consider in reference to cybersecurity, are the following:

1. Companies need to realize that there are risks. Everywhere. Every company can be targeted, and that truth has to be accepted. There is no time for ignorance.
2. Important company assets need to be identified, in order for the company to know what needs to be protected and how it should be protected.
3. Personnel in charge of cybersecurity, who will prioritise these questions, is vital. If the company does not have knowledgeable personnel, a professional partner could be
the solution. Either way, people who are experienced and knowledgeable in the area of cybersecurity will be of great benefit for the company in the future. In line with this, the issue of safety must have its own bullet point on the agenda during company meetings.

4. Run background checks! It is important to have a complete understanding of who companies hire, especially when it comes to critical positions, such as employees with access to important company systems, for instance.

5. Continuously testing of company systems is an vital aspect, in order to realize if everything works the way it should. That, in turn, minimizes risks for the company.

4.2.2 Magnus Lindegren, Swedish police superintendent and head of frauds

Magnus Lindegren is a Swedish police and head of frauds in Western Sweden, which includes Västra Götaland and Halland. He and his staff manage different types of crimes, where four specific crimes are more prominent: frauds, embezzlement, allowance crimes and disloyalty to principal. Their work includes both analogue and digital crimes, and the most common crime they encounter is called CNP (card not present). This crime is explained as an individual getting credit card details stolen and used by someone else.

“My responsibility is to make sure that my staff is comfortable enough to perform their best at work. Another part of my job is to hold lectures in the field of security and risk management, which is a lot of fun. I like to teach people and companies about this, in order to decrease the crimes. Our goal with the lectures, is to prevent crimes from being completed. If companies know how to protect themselves, it won’t be worth it for criminals to keep committing crimes.”

Magnus interest in cybersecurity started around 2007, when he worked as a squad commander at Hisingen in Gothenburg. Him and his team were managing frauds already back then, but not as many digital frauds as today. Digital frauds have definitely increased, Magnus means, which has created problems for the police today. Magnus encounters both companies and individuals, who have been exposed to digital frauds. The most companies he meets are fairly young and new on the market, but have experienced a great growth during a short period of time. These companies have a harder time keeping up with the development
of frauds.

Even though Magnus says cybersecurity is fairly prioritised amongst companies today, there is still a gap between thought and action. He explains security and safety to be associated with cost, whereas companies rather would focus on income and sales instead of security, which would imply costs. He also assumes companies to be afraid of losing customers if the actual purchase takes too long because of an extra filter of safety in the purchase process. Thus, companies choose not to focus on security. Another reason, according to Magnus, could be the payment solutions and choice of allowing another company to be in charge of these. If a fraud would occur, the payment company would instead take the fall. Overall, Magnus means that companies today do not care about possessing knowledge in cybersecurity; their driving force is to make money.

“I honestly think companies think more about money than knowledge. We meet different security departments from different companies, who all say the same thing: the board of directors only want to make money and sell goods. They don’t care about what the security department says, and are more interested in revenue instead of safety.”

Magnus has three expert tips for online companies:

1. Time is always of benefit for the one committing the fraud! Short lead times is not beneficial in terms of security, where Magnus mentions short lead times to decrease the company’s ability to review the placed orders to find possible frauds. He also stresses the importance for online companies to use 3D-secure, which forces the customer to identify him-/herself during the purchase process, which makes it more difficult to commit frauds.

2. A buying limit of the company’s own choice is necessary when selling electronics or expensive brands, for example. Thus, all orders exceeding the pre-decided buying limit should be more closely reviewed.

3. If companies started saving IP addresses, the police’s detective work would be easier when frauds occur. Even though different identities are used, they might occur at the same IP address, which could tie one person to different frauds.
Additionally, Magnus general advice for companies is to assess and better view what they are risking. He proposes all companies to make a risk analysis with both internal and external aspects. Additionally, he would like online companies to aim a little higher and work by the same standards, in order to jointly decrease online crimes.
5. Analysis & Discussion

In this part of the thesis, the results are analysed relative to previously mentioned conceptual framework, as the analysis will follow the same manner as the theory of The cyber risk management process. Thus, the headings included in the process will be used to analyse all gathered data, both primary and secondary, in a meaningful way. In addition to this, the author’s own thoughts will be discussed simultaneously.

In order to answer the purpose of investigating how cybersecurity is managed in Swedish online fashion companies, the results from the interviews will be analysed and discussed below. Answers to the research questions can be found as well.

1. Risk identification

Two of the companies clearly stated cybersecurity to be of importance, since e-commerce is a vital part of the companies’ business. The third company solely described a visual presence of cybersecurity, but not the prominence. Personal financial information and sensitive customer information were mentioned by one company to be key reasons for the presence of cybersecurity. Despite of what the online fashion companies say, both of the cybersecurity experts saw cybersecurity as more or less unprioritised amongst companies today. This was mentioned to be a result of lack of knowledge as well as companies’ focus tend to be placed more on income instead of costs, which security and safety often are associated with. One of the cybersecurity experts actually mentioned companies to rather make money instead of understanding the field of cybersecurity better. In line with this, MacDonnell (2014) proposed companies to implement cybersecurity as a way of enhancing the company’s overall risk management. Thus, companies need to understand that spending money on cybersecurity is an investment in the company.

Interestingly, only one company described a company model to be used when identifying risks. Waters (2011) means that it is important for a company to have a stated risk identification process when identifying risks in order to better review uncertainties in a supply chain and thus identify the most significant associated risks. However, all three companies recognized respectively website as a valuable firm asset, which is in line with
Kosub (2015) and Abnett (2016), who mentioned online companies to be more exposed to cyber risks, since their entire business can be found online. As online shopping is estimated to grow in the near future as well, having a robust and stable website would be considered important too. In line with this, one of the cybersecurity experts commented on companies ability to recognize valuable firm assets. He mentioned the difficulty of identifying company risks if valuable firm assets were unidentified. Additionally, identifying valuable firm assets will help the company to know what needs to be protected and how this should be done. This is mentioned by both Kosub (2015) and Refsdal et al. (2015) as well, who explain a correct asset identification to be one of the key challenges for companies when properly assessing cyber risks. Two out of the three online fashion companies seemed to have a fairly good idea of how to identify valuable firm assets, but the processes somehow do not feel complete. Perhaps not all the information regarding this was revealed during the interview, which in that case would explain the ambiguity. Tentatively, the companies could spend some extra time on identifying valuable firm assets to get an even more accurate cybersecurity.

Trespassing on the website was explained by one company to be the most common cyber risk, whereas the other two companies had no knowledge of previous cyber risks the company has been exposed to. MacDonnell (2014) and Refsdal et al. (2015) mean that more or less every company somehow has been exposed to cyber risks, but most companies are unaware of it. Overall, none of the companies mentioned a sat budget for the cyber risk management, and solely one company had invested in personnel specifically in charge of cybersecurity questions. This is underlined by Khojasteh (2018) and one of the cybersecurity experts to be of importance, in order to put emphasis on the field of cyber risk management. For the future, hiring people with experience from and knowledge in cybersecurity is mentioned by the same expert to be very beneficial for a company. Furthermore, all three online fashion companies somewhat mentioned knowledge to be of importance when identifying risks: knowledge about previous cyber risks, knowledge about upcoming cyber risks as well as knowledge about current, flourishing cyber risks were aspects brought up. Refsdal et al. (2015) also explained more knowledge about possible risks to result in more accurate identifications. This is in line with what one of the cybersecurity experts mentioned, that companies unawareness of their risks results in ineffective company risk management.
According to said expert, the biggest reason for unawareness is the lack of risk analyses performed at the company.

Even though all of the online fashion companies stressed the importance of knowledge and experience in cybersecurity, one of the companies specifically expressed a view of an overall lack of knowledge amongst today’s online companies. Digitalisation and cybersecurity are seen to be that important nowadays, which made it hard for this one online fashion company and one of the cybersecurity experts to understand why companies, especially online companies, today do not put more effort into this. Rumsey (2016) and Trautman (2017) too mentioned lack of knowledge to be the reason for the non-prioritisation. If companies, especially board of directors and people with power at the company, understood cybersecurity and the accompanied risks better, perhaps there would be a paradigm shift and cybersecurity would be more prioritised.

Finally, one of the cybersecurity expert meant that companies might disregard cybersecurity if another company is in charge of the customer payments, as the severity of monetary risks might not be considered to be as important. If another company would take care of possible monetary losses, the company itself would never have to consider upscaling the security in order to not be exposed to this, as the exposure is minimum. Only one of the online fashion companies mentioned outsourced payment solutions, whereas the other two companies did not refer to this at all. Perhaps this outsourced payment solution is seen as a safeguard from not only frauds, but also spending money on a increased cybersecurity.

2. Risk assessment and valuation

When assessing and evaluating risks, all of the companies mentioned company size, in these cases a smaller company, as a reason and explanation for not being targeted and exposed to cyber risks. This is contradictory to what Refsdal et al. (2015) and Trautman (2017) said, who instead meant that any company can be targeted by cyber criminals, regardless of size. One of the cybersecurity experts even mentions both big and small companies to be in need of an accurate cyber risk management! However, the other cybersecurity expert described “younger” companies to be struck harder by cyber risks, as the development of cyber frauds
move quicker than companies’ understanding and knowledge. Perhaps this does not have to be the case. If a younger company better understands today’s digital environments in comparison to older, more stubborn board of directors, who want to continue like they always have, this younger company would gain an advantage. As long as companies are enlightened about cybersecurity and all of today’s possible risks, perhaps it does not matter if the company is young or old. Knowledge could instead be seen as the key here.

All online fashion companies somewhat assessed the likelihood of different cyber risks to happen, where one company explained new and upcoming cyber risks to be frequently raised at company meetings. If the cyber risk was considered an immediate threat towards the company, actions were taken. This is in line with what Kosub (2015) said, who highlighted the importance of management to decide whether the risk is acceptable or if specific measures have to be implemented. This should be done prior to an eventual exposure to the cyber risk, which one of the cybersecurity experts also stress. Waters (2011), Kosub (2015) and Khojasteh (2018) all agreed and mentioned proactive solutions to be the best solutions. In line with this, another online fashion company mentioned knowledge about previous cyber risks to be used as proactive solutions for the future. Basically all researchers and the two cybersecurity experts agreed on the better the knowledge, the better the solutions.

Refsdal et al. (2015) mentioned the importance of understanding how difficult it could be for unauthorized people to penetrate company systems and reach sensitive assets. One fashion company described specific penetrations tests, both of the company’s systems and the guest network. This was proposed by one of the cybersecurity experts, who mentioned red teaming exercises as a solution to help the management understand what shortcomings there are in the company as well as in the systems. Interestingly, penetration tests were not mentioned by any of the other two companies. However, another fashion company did mention risk assessment for every system to be implemented on a regular basis. One of the cybersecurity experts gave further advice for companies to continuously test company systems, in order to realize if something were to be wrong. Discovering this in time, minimizes unnecessary risks. Two of the three online fashion companies seemed to have a fairly good view of how respectively company’s systems worked, and how well they were protected. However, not everything was uncovered during the interviews, which could imply “holes” and shortages in the systems.
Knowledgeable personnel, external or internal at the company, should definitely be in charge of this, in order to perform as accurate testings as possible.

3. Risk response

Two out of three online fashion companies mentioned security systems at the website as a risk response, where firewalls were brought up as an example. This is explained as risk mitigation (Kosub, 2015), risk reduction (Refsdal et al., 2015) or as risk prevention (Khojasteh, 2018), where all terms refer to the same thing: a company paying another company to take preventive measures in order to reduce the probability of different cyber risks to occur. Waters (2011) mentioned the benefits of getting help from knowledgeable partners when the company’s own knowledge is scarce. Partnering with another, more experienced company might increase the feeling of security at the company. This could further give the company a sense of not being all alone, but instead having someone to share ideas and concerns with. Risk mitigation could be seen as one type of risk transferring (Kosub, 2015) or risk sharing (Refsdal et al. 2015); in this case, the risk is transferred to the suppliers and the company more or less stands beyond responsibility. The last online fashion company, the one owned by the bigger, global fashion company, mentioned blocking of certain web pages in order to avoid risks. As this can be seen as risk mitigation, their entire risk response process could be explained as risk transferring: the global fashion company is completely in charge, and thus takes all the possible downfalls.

Interestingly, only one online fashion company explained a pre-decided risk management model to follow when responding to risks. Waters (2011) underlined the significance of preparations made by the company, in order to better know how to respond to the risks. Perhaps a pre-decided risk response model would help every company in stressful and critical situations. Instead of wasting energy and time on thinking of solutions when something were about to happen, instructions are solely followed. One pre-decided response to every type of risk would thus be ideal. However, if there are suppliers taking care of the initial responses to risks, i.e. risk transfer (Kosub, 2015) or risk sharing (Refsdal et al., 2015), a pre-mapped out risk response model might not be as important. Risk transferring is implemented by two out of three online fashion companies, which could explain their notably lower prioritisation of this part of the process.
Knowledge was apparent also in this part of the process, where one online fashion company mentioned difficulties of responding to risks if the risk and the damage is unknown. Refsdal et al. (2015) mentioned knowledge about the possible risks to result in more accurate responses. This is in line with what another online fashion company mentioned, who underlined experience from previous risks to help decide on more precise responses in the future. This can be done in order to reduce the likelihood of that same cyber risk to happen again, which Refsdal et al. (2015) explained as risk reduction. A company working closely to another, more experienced company could perhaps experience an enhancement of cybersecurity knowledge, where learning is part of the process.

4. Risk control
Two out of three online fashion companies understood the importance of monitoring risks and risk responses for improvement and a more accurate risk handling in the future. One of the two companies always evaluated and reviewed a cyber attack immediately after an incident occurred, and then relied on this knowledge for the future. The other company mentioned annual digital audits as well as a constant reviewing of risk factors. Waters (2011), MacDonnell (2014) and one of the cybersecurity experts explained online fraudsters to become increasingly intelligent in their work, which requires companies to constantly review and monitor their cyber risk management. Companies need to “keep up” with new cyber risks, in order to choose the best responses. This goes hand in hand with knowledge: the more knowledge about cyber risks, the more accurate the responses and the risk handling will be. This could be seen as part of an holistic cybersecurity at the company; it is not just about identifying risks or responding to risks, the company also needs to see and understand “the bigger picture” for future risks, responses and an overall better control.

5. Risk culture and risk government
More or less all three online fashion companies mentioned a rich risk culture at respectively company. One company mentioned online courses in risk management to be mandatory for all new employees to complete. The other two companies mentioned GDPR (General Data Protection Regulation), which is the new updated information security policy. This seemed to be taken very seriously, as both companies were educating the staff in these questions. One
company actually brought in expertise when compiling the new policy. Kosub (2015) underlined training of all employees to be of great importance, since different actions of people and user faults often result in unnecessary cyber incidents. Perhaps companies could minimize unnecessary slips if the staff is properly educated in what they themselves can do in order to avoid exposing the company to different cyber risks.

Two online companies mentioned an in-house access team to be in charge of all employees having the right access to different systems, and that it works correctly. This is a great way of keeping track of what every employee is permitted to access. In line with his, one cybersecurity expert mentioned running background checks of people before hiring them, to be vital. Imaginable, it is not only important to know about people's’ previous knowledge in cybersecurity to benefit the company in the future, but it could perhaps also be important to know what companies they have worked at before, if they have criminal records and so on. Employing the wrong person at critical positions with a lot of company access could indeed be devastating for the company. No one can know beforehand if a person is there for the wrong reasons, i.e. to steal sensitive company information, for instance.

Interestingly, only one online fashion company mentioned the wireless network and the guest network to be critical parts of their cybersecurity. Visitors could connect to the guest network, as the company was sure no sensitive company information could be reached through that network. However, interns could connect to the regular wireless network without any specific measurements. This could as well be critical, since interns most often only stay a shorter period of time at a company, and so the turnover of interns is high. That could result in a lot of unauthorized people accessing all kinds of company systems and sensitive information. Perhaps it could be mandatory for all interns to sign an agreement or go through an risk education, to know what is acceptable and not at the company.

To conclude the analysis and discussion
When analysing and discussing the results from the interviews, three areas appeared to be the most prominent. These are described below.
1. Knowledge
Knowledge (or perhaps the lack of knowledge) was eminent in all parts of the process. Whether it was about understanding risks, identifying valuable company assets, understanding the right risk responses or predicting upcoming risks, knowledge seemed to be the key. It is difficult for a company to identify risks if valuable company assets are not understood. It is difficult for a company to respond to risks, if the risks are not understood. It is difficult for the employees at a company to understand risks, if the higher management cannot mediate these risks in a proper way. More or less all previous researchers, all online fashion companies as well as both of the cybersecurity experts agreed on the better the knowledge, the better the solutions and the better the cyber risk management.

2. The importance of cybersecurity and cyber risk management
Neither I nor previous researchers can stress the importance of cybersecurity and cyber risk management any clearer - companies need to start taking this seriously! There are cyber risks, there will always be cyber risks and any company can be targeted. Recognizing the prominence and importance of cybersecurity is vital for any company’s future development. There will be new cyber risks and fraudster will become even smarter in their work, which makes spending money on cybersecurity a necessity rather than an expense.

3. The holistic view
Finally, the holistic view has to be brought up. Several researchers firmly stress the holistic view of cyber risk management, where all parts of the process is given the same amount of attention. Understanding risks and identifying valuable company assets are absolutely important for a company, but it will not benefit the bigger picture unless suppliers, partners and employees also understand the severity of cybersecurity and cyber risks. For instance, allowing a couple of employees to be in charge of these questions is important for cybersecurity to be taken seriously at company meetings. GDPR seemed to be prominent this year as well, which highlights the matter of cybersecurity even more. Educating the staff in GDPR could be a first step for every company to reach a more holistic cyber risk management view.
6. Conclusions & Future research

Through semi-structured interviewing, knowledge of how cybersecurity risks are managed in Swedish online fashion companies was gained. Additional information of whether or not cybersecurity is being prioritised in Swedish online fashion companies as well as how Swedish online fashion companies handle cyber risks was uncovered too. Thus, both the purpose and the research questions were answered.

To conclude this study, information showed a fairly well current management of cybersecurity risks in Swedish online fashion companies, where companies attempt to work proactively. Cybersecurity is prioritised amongst these companies, but perhaps not on a preferable level. The companies’ cybersecurity could definitely benefit from more attention. Hence, knowledge in the field should be increased and thus, a better holistic view could be implemented. Here, companies would benefit from having one group of people in charge of these questions. The importance of cybersecurity is gaining increased attention, but sadly still remains unprioritised by management teams and board of directors. This further creates difficulties for the rest of the employees to comprehend the severity. Hopefully, the new policy of GDPR could shed more light on the importance.

This paper contributed to the overall knowledge in the field of cybersecurity, which could be applied to any online company, but is probably less applicable to offline shopping. The three previous mentioned areas could work as springboards for future research, where also social engineering risks should be considered. The aspect of social engineering risks was touched lightly upon during the interviews, but not elaborated specifically further. Perhaps this is a field in need of future research, in order to determine the risk level and if prioritization amongst companies might be necessary.

Even though contribution to the theoretical and practical field of cybersecurity was made, scarcity of company information might have affected the outcome. This could be a result of companies’ unwillingness to reveal too much sensitive information or interview questions lacking deep.
7. Managerial implications

The chapter of managerial implications gives further suggestions on what online fashion companies can do in order to attain a higher level of organisational cybersecurity.

- First of all, companies need to recognize the importance of cybersecurity and understand that all companies are possible targets. When this realization is reached, it will be easier for the company to detect more practical solutions.
- When identifying risks, companies should start by identifying valuable firm assets in need of protection. This knowledge will facilitate the risk identification process.
- Increase the overall organisational knowledge in the field of cybersecurity and educate all employees at the company. The more knowledge the employees have, the higher will the level of attained company cyber risk management be.
- Assign one said group of people at the company to be in charge of cybersecurity questions. This group should be the driving force in placing cybersecurity on the agenda at company meetings.
- Companies need to understand that spending money on cybersecurity, whether it concerns knowledgeable partners to collaborate with or education of the staff, is a long-run investment in the company and not a loss of capital.
List of references


Carlsson, B. (1991) Kvalitativa forskningsmetoder, (In English: Qualitative research methods), Almqvist & Wiksell Förlag AB.


Accessed through the University of Borås’ library <www.hb.se/biblioteket> (Retrieved 2018-04-16)


Appendix 1: The interview guide for online fashion companies, step by step

Before the interview

- **Introduction**

To begin with, I would like to ask if you feel comfortable with me recording our interview and your answers. If that is okey, I will start the recorder now. First of all, I want to make sure that you understand the purpose of my thesis and the goal with this interview. The purpose for this study is to “investigate how cybersecurity is managed in Swedish online fashion companies”. Thus, I would like to understand if cybersecurity is prioritised in today’s Swedish online fashion companies, and how cyber risks might be handled. In order for you to be able to answer my questions, I need to make sure that you understand the concepts of risk management, cyber risk management and cybersecurity in the same way as presented in this thesis. Risk management can be described as an organisational process, where activities, such as identifying, analysing and responding to risk, are performed. Cyber risk management is closely related to risk management, but here, the risks are caused by cyber threats instead. The process in cyber risk management, contains identification of risks, evaluation of risks and responding/treatment of risks. Finally, cybersecurity refers to the security of a system, in order to avoid a cyber threat. That is, protecting any electronic information, the communication technology it depends on as well as the cyberspace-users.

This interview will be conducted in three steps. First, I will ask you some personal questions. Secondly, I will ask questions about the company’s current risk management, cybersecurity as well as the cyber risk management process. Finally, safety questions about the personnel will be asked. In total, 15 questions will be asked. The interview will last maximum of one hour, depending on your level of interaction and answers.

**During the interview**

- **Personal questions**

In this part, the interviewee will be asked some personal questions, in order for me to better get to know the person as well as to understand previous and current work positions. It is important for me to understand if cybersecurity has been prioritised during previous years, which hopefully will give answers to when cybersecurity began being interesting and
important for online fashion companies. It is also important to understand the interviewee’s part in the company’s risk management. Is he/she him/herself involved in this enough to give accurate answers? If the respondent does not feel comfortable revealing name and/or workplace/company, I will continue the interview anonymously and consequently remove question 1.

Q1: What is your name and what is your job position?
Q2: What are your main work tasks?
Q3: For how long have you been working here?
Q4: Have you had similar jobs before? In that case, did you have similar/the same work tasks?

- **Questions about the company today**
In this part, the interviewee will answer questions about the company’s current cyber risk management and cybersecurity. These questions are connected to the cyber risk management process, which hopefully will provide me with pieces of the company’s process. Question 10 is a complementary question, only asked if there is inconsistency between theory and the interviewee’s answers.

Q5: What kind of risk management is performed at the company? How involved are you?
Q6: To what degree is cybersecurity prioritised at the company?
Q7: How do you assess the company’s cyber risks? Is the company very, fairly or not at all exposed to cyber risks?
Q8: What kind of cyber risks are the most common for the company? What is the likelihood of these happening?
Q9: How does the company respond to cyber risks and threats, if they would occur?
Q10: Could you please walk me through the company’s cyber risk process. From establishing of cybersecurity to treatment of cyber threats.
Q11. Has the company had any exposure to cyber threats recently? If yes, what happened and what did you do?
• **Personnel safety questions**

The personnel plays a big part in protecting the company against exposure of unnecessary risks. Thus, this part will be dedicated to a dialogue about personnel safety questions in order to gain knowledge about staff education and if this is something the company finds important.

Q12. Does the company have specific personnel in charge of risk management, specifically cyber risk management? If yes, what is this personnel’s main tasks?

Q13. To what degree is the rest of the company’s staff educated and knowledgeable in risk management, cyber risk management and all of the accompanied parts of the processes?

Q14: To what degree is the company’s staff educated in what they themselves can do when it comes to avoiding cyber risks?

During the interview, I will audiotape (with consent from the interviewee) as well as take notes.

**Conclusion**

• **After the interview**

I will thank my interviewee for taking his/her time to meet me and answer my questions as well as ask if there is something he/she would like to add. To end the interview, I will offer the interviewee the opportunity to read my thesis once it is finalized.

Q15: Is there anything you would like to add?

After the interview is completed, I will listen to the recording and fill in notes from what might have been overlooked during the interview. When this is done, I will transcribe the interview in order to easier analyse it. If necessary, a follow up conversation will be conducted and send by email later on. This conversation will not include any questions, but rather be a summary of what was said during the interview. This summary should be approved by the interviewee, in order to determine the accuracy of the interview.
Appendix 2: The interview guide for cybersecurity experts, step by step

Before the interview

- Introduction

To begin with, I would like to ask if you feel comfortable with me recording our interview and your answers. If that is okey, I will start the recorder now. First of all, I want to make sure that you understand the purpose of my thesis and the goal with this interview. The purpose for this study is to “investigate how cybersecurity is managed in Swedish online fashion companies”. Thus, I would like to understand if cybersecurity is prioritised in today’s Swedish online fashion companies, and how cyber risks might be handled. Your expert knowledge will help me to better understand what these companies should be doing and what they should think about when it comes to cybersecurity. In order for you to be able to answer my questions, I need to make sure that you understand the concepts of risk management, cyber risk management and cybersecurity in the same way as presented in this thesis. Risk management can be described as an organisational process, where activities, such as identifying, analysing and responding to risk, are performed. Cyber risk management is closely related to risk management, but here, the risks are caused by cyber threats instead. Finally, cybersecurity refers to the security of a system, in order to avoid a cyber threat. That is, protecting any electronic information, the communication technology it depends on as well as the cyberspace-users.

This interview will be conducted in three steps. First, I will ask you some personal questions. Secondly, I will ask questions about how you, through your job, experience companies’ current cyber risk management and cybersecurity. Finally, the last questions will cover your view of what companies should be doing as well as your expert tips. In total, eight questions will be asked. The interview will last maximum of 30 minutes, depending on your level of interaction and answers.

During the interview

- Personal questions

In this part, the interviewee will be asked some personal questions, in order for me to better get to know the person as well as to understand their current work position. It is important for
me to understand what the interviewee’s main work tasks are and how knowledgeable he/she is in the field of cyber risk management and cybersecurity, in order to determine the level of accuracy of the answers. If the respondent does not feel comfortable revealing name and/or workplace/company, I will continue the interview anonymously and question 1 will be removed.

Q1: Please state your name and current work position.
Q2: What are you main work tasks?

- **Questions about own experience of cyber risk management and cybersecurity**

In this part, the interviewee will answer questions about the daily job experience of companies’ current cyber risk management and cybersecurity. These question will help me understand when cybersecurity became important enough for companies to consider expert help and knowledge.

Q3. When did your interest for cybersecurity and cyber risk management emerge?
Q4. What kind of companies do you encounter in your daily work?
Q5. To what degree would you say cybersecurity is prioritised amongst companies today?

- **What companies should be doing as well as expert tips**

In order to understand what companies should be doing, they need to map out their weaknesses and lack of knowledge. Answers to these question will hopefully provide me with additional information for my own, theoretical model, consisting of what companies should do and think about in the field of cybersecurity.

Q6. Where do companies lack knowledge? What should be considered?
Q7. What are your expert tips to companies operating online?

During the interview, I will audiotape (with consent from the interviewee) as well as take notes.
Conclusion

- **After the interview**

I will thank my interviewee for taking his/her time to meet me and answer my questions as well as ask if there is something he/she would like to add. To end the interview, I will offer the interviewee the opportunity to read my thesis once it is finalized.

Q8: Is there anything you would like to add?

After the interview is completed, I will listen to the recording and fill in notes from what might have been overlooked during the interview. When this is done, I will transcribe the interview in order to easier analyse it. If necessary, a follow up conversation will be conducted and send by email later on. This conversation will not include any questions, but rather be a summary of what was said during the interview. This summary should be approved by the interviewee, in order to determine the accuracy of the interview.