UNIVERSITETET I AGDER

The Impact of Digital Vulnerabilities on Organizational Resilience

A case study of different perceptions in a supply chain

LILLY A. HAUGSEGGEN
& HENRIK G. FAUSKE

For the Master's Degree in
Industrial Economics and Technology Management

SUPERVISOR
Gøril Hannås

University of Agder, 2019
Faculty of Engineering and Science
School of Business and Law

I. Preface

This master thesis is written as the final report of our Master Program in Industrial Economics and Technology Management at the University of Agder, concluding our M.Sc. degree. It is written during the 2019 spring semester and represents 30 credits.

The study aims to investigate how digital vulnerabilities present in supply chains impact organizational resilience. We found it interesting to look at how perceptions differs from each tier in a supply chain and were exited to learn that DNV GL would allow us access to some of their clients' projects. The topic of the master thesis was selected based on our mutual interest in industrial supply chains, and furthermore how digitalization requires the business world to think differently.

Working on this thesis has been challenging at times, as there is not a lot of research conducted on the combination of digital vulnerabilities and organizational resilience. On the other side, it has been both exciting and rewarding to investigate a rather new area. We would like to give a special thanks to our supervisor Associate Professor Gøril Hannås for valuable guidance and constructive feedback. A sincere thanks to Professor Omera Khan for crucial inputs and discussions. On behalf of DNV GL, Boye Tranum have given us a rare chance at looking into a four-tier supply chain, in addition to promoting our creativity when we have struggled. We are highly appreciative for his contribution. Finally, would I, Lilly, express my gratitude to my beloved grandmother who unexpectedly passed away during the final week of writing this thesis. She has wholeheartedly supported me throughout my studies and been an inspiration to me.

Høvik, May 2019

Lilly A. Haugseggen

Henrik G. Fauske

II. Summary

Digitalization has led organizations to be more effective and cost efficient. However, it has also brought new sets of vulnerabilities. Digital vulnerabilities can occur from technology, such as bugs or malfunction in software, or from human interaction with technology. These vulnerabilities could originate from either intentional or unintentional actions and reduce an organizations' resilience if appropriate capabilities are not constructed. These capabilities are considered to be an organizations' skill to achieve its ambiguous goals.

This thesis aims to investigate how digital vulnerabilities impact organizational resilience by posing three research questions. These are answered by conducting a case study of a four-tiered supply chain, performing qualitative interviews backed up by a literature review. It identifies key digital vulnerabilities present in a supply chain and the consequences of ignoring them. Furthermore, a comparison of different perceptions of *digital vulnerabilities* and *organizational resilience* is given and guidance on future organizational resilience is presented.

Our findings highlight the extensive use of e-mail and flow of information as the most significant source of digital vulnerabilities. Exchange of sensitive documentation with unknown recipients reduce the oversight of who obtains information, consequently leading it to fall into the wrong hands. Considering differences in perceptions, does the main distinction occur between the third and fourth tier. The first three tiers are aware of their possibility of being attacked, while there is a general belief among the fourth tier that unfortunate events do happen, but not to them.

A supply chains common goal of staying resilient is challenged by the tiers having different understandings and ways of handling digital vulnerabilities. The smaller organizations were not pointed out as the weakest link. However, our findings show that they are a bigger threat to the supply chain than they are aware of. A denying attitude toward digital vulnerabilities will potentially damage organizational resilience if they are not properly managed.

Table of Content

List of Figures

List of Tables

1 Introduction

The digital sharing of information within modern supply chains is crucial to be able to make decisions in a constantly changing environment, where organizations rely on accurate and up to date information. However, digitalization is argued to make organizations increasingly vulnerable to cyber-attacks, by creating an environment of unknown risks (Harteis, 2018; World Economic Forum, 2017).

Cyber-attacks are becoming more usual than ever before and rises threats to our modern digital society. Ever since the first reported cybercrime in 1973 within the Union Dime Savings Bank it has been continually evolving (K. Huang, Siegel, & Stuart, 2018). Recently, Norsk Hydro experienced a cyber-attack that paralyzed parts of their operations and reported a loss of approximately $50 million (Hovland, 2019). Morgan (2016) states the importance of cybercriminal activity as one of the biggest challenges that humanity will face in the next two decades, by referring to Cybersecurity Ventures prediction that the cost of cybercrime will increase from $3 trillion in 2015 to $6 trillion dollars by 2021.

Digital disruptions can penetrate and impact every company in a shared network, making the supply chain only as resilient as its weakest link (Estay & Khan, 2015). Organizations does not only impact their own level of resilience, but also the level of resilience of their customers, suppliers and the overall shared digital environment (World Economic Forum, 2017). Organizations therefore needs to be aware of the potential threats they can encounter and prepare for how to deal with them. The new digital era of supply chains require that organizations become more resilient, especially against digital vulnerabilities as the methods used for exploiting these are getting cheaper, more effective and are in constant development (PST, 2019).

This study aims to investigate how digital vulnerabilities present in supply chains impact organizational resilience, by the following research objectives:

1. Identify and categorize key digital vulnerabilities present in supply chains
2. Investigate potential consequences of digital vulnerabilities
3. Compare different perceptions of *digital vulnerability* and *organizational resilience* in a supply chain

4. Form supporting tools to help improve organizational resilience in digital supply chains based on key drivers for digital resilience

These research objectives will be met by answering the following research questions:

1. What are the key digital vulnerabilities impacting modern supply chains and what are the consequences of ignoring these vulnerabilities?
2. Are perceptions of *digital vulnerabilities* and *organizational resilience* different from each tier in supply chains?
3. How may an increased focus on organizational resilience reduce the impact of digital vulnerability?

To be able to answer the research questions we will conduct an embedded case study of six organizations within four tiers of a supply chain. In this study we do not consider technical vulnerabilities, such as the quality of firewalls and antivirus programs. Instead we want to look at the perceptions of how digital vulnerabilities affect organizational resilience, implying that we will investigate on a human and organizational level.

2 Theoretical Framework

Organizations operating in the same supply chain have encountered radical changes of interaction and collaboration due to digital technology and inter-organizational information systems. Traditionally, supply chains were designed to focus on the movement of materials, rather than flow of information (Ramanathan, 2014). Organizations are sharing information mainly digitally and they are dependent on rapid, quality information to be able to make the right decision in a fast pace environment (Khan & Estay, 2015). Moreover, there is a need for the companies to exchange information at a faster pace than before to stay competitive since their working environment is becoming increasingly more globalized and therefore calls for the need to get more information to stay competitive. Because of this, supply chains have become more vulnerable in an interconnected, volatile and global economy, where even minor disruptions can cause significant financial losses (Fiksel, Polyviou, Croxton, & Pettit, 2015).

Traditional handling of risk has included risk identification, risk impact evaluation, risk prioritization and preventive action towards making sure the risk doesn't occur or mitigate the level of it. Modern supply chains are becoming more complex and creates modes of failure beyond the risks that organizations are capable of handling with these tools. It is becoming more difficult to foresee every possible way an organization or supply chain can be disrupted (Estay & Khan, 2015). Organizations could be sleepwalking into disaster if they do not find out how to manage and sustain resilience in their organization (Denyer, 2017).

2.1 Resilience Thinking

The traditional way of coping with adverse events, is to identify risks by analyzing the past and predicting the future (van der Vegt, Essens, Wahlström, George, & Som, 2015). This approach may help to anticipate and mitigate some of the consequences. Traditional risk management is helpful for familiar threats but has severe limitations in a world of turbulent change and unforeseen black swan events (Fiksel, 2015). According to van der Vegt et al. (2015) there is a shift in attention; from identifying and mitigating risk to trying to increase resilience. Whereas the concept of risk tends to dwell on the downside risks, risks to be avoided and ideally eliminated, upside rewards are equally relevant to resilience thinking (Fiksel, 2015).

Resilience is both a function of the vulnerability of a system and its adaptive capacity (Dalziell & McManus, 2004). Yosef Sheffi (2005) considers resilience for companies as a measure of ability, and the speed at which they can, return to normal performance level following a disruption that is of low probability but with high impact. Inability to characterize such disruptions is according to Kunreuther (2006) the greatest weakness of risk management.

The term *resilience* was first used in 1973 by Holling, with the work title "Resilience and Stability of Ecological Systems". He finds that the resilience and stability viewpoints of the behavior ecological systems have very different approaches to the management of resources, and that a management approach based on resilience would emphasize the need to keep options open and be receptive to heterogeneity. Resilience as a concept is claimed to be discipline specific (Bhamra, Dani, & Burnard, 2011; Ponomarov & Holcomb, 2009). In their review of resilience literature, Bhamra et al. (2011) look at interdisciplinary perspectives of the concept of resilience. Resilience can be put in contexts such as physical systems, ecological systems and disaster management. The definitions include key elements like returning to equilibrium, absorbing change and disturbance, magnitude of disturbance that a system can tolerate, ability to mitigate hazards and minimizing disruption. To summarize, Holling (1973) operationalizes the term as a system's capability to absorb changes. Continuing, resilience adapted into different directions, amongst them are supply chain resilience and organizational resilience.

2.1.1 Supply Chain Resilience

Supply chain resilience is defined by Ponomarov and Holcomb (2009) as *"the adaptive capability of the supply chain to prepare for unexpected events, respond to disruptions, and recover from them by maintaining continuity of operations at the desired level of connectedness and control over structure and function".* Christopher and Peck (2004) includes agility as an important factor to supply chain resilience by highlighting the ability to respond rapidly on unpredictable changes. Ultimately, a supply chain will only be as resilient as its weakest link (Estay & Khan, 2015), as the overall resilience of a supply chain is dependent on the participating organizations' resilience and their ability to manage their individual corporate risks.

Some argue that supply chain resilience can be interpreted as a part of organizational resilience, and that elements of supply chain risk management are part of organizational resilience (British Standard Institution (BSI), 2014). Existing definitions on resilience, supply chain resilience and

organizational resilience are often interchanging, or contractionary and confusing (Ponomarov & Holcomb, 2009). The definitions and concepts are overlapping each other, and they are not always easy to distinguish. Therefore, in the context of this thesis, a stand point has been taken. We will argue that supply chain resilience and organizational resilience are two interconnected phenomenon that are mutually dependent on each other. Just like every organization is a citizen of its supply chain (Yossi Sheffi & Rice, 2005), supply chains are dependent of the participating organizations.

2.1.2 Organizational Resilience

Historical View of Organizational Resilience

The term "resilience" was first used in 1973 by Holling as stated above. However, Meyer (1982) was one of the first to put the term resilience in an organizational context, while studying how hospitals handled doctors on strikes. The term "resiliency" was used to describe the organizations ability to tackle these sudden disruptions and restore order after the strikes ended. According to Denyer (2017), organizational resilience has been split between two core drivers over time; a progressive approach and a defensive approach. The progressive approach focuses on searching for problems and opportunities, to solve them and prosper. The defensive approach focuses on stopping problems when they happen and where no actions are taken before the problem occurs. In his findings, he states that organizations' main focus has been on the defensive part. The focus has been on designing resilient systems that consists of making operating procedures, certification and competence as optimal as possible and by doing so, not focusing enough on tackling new possible threats or exploiting new opportunities. However, during the latest years a more progressive focus has evolved and become important for modern organizations.

The following timeline in Figure 2.1 shows how organizational resilience have evolved over the last 40 years and how new elements have been included in the way of thinking. The timeline data originates from Denyer's review on organizational resilience and are cross-checked with elements from Ponomarov and Holcomb (2009).

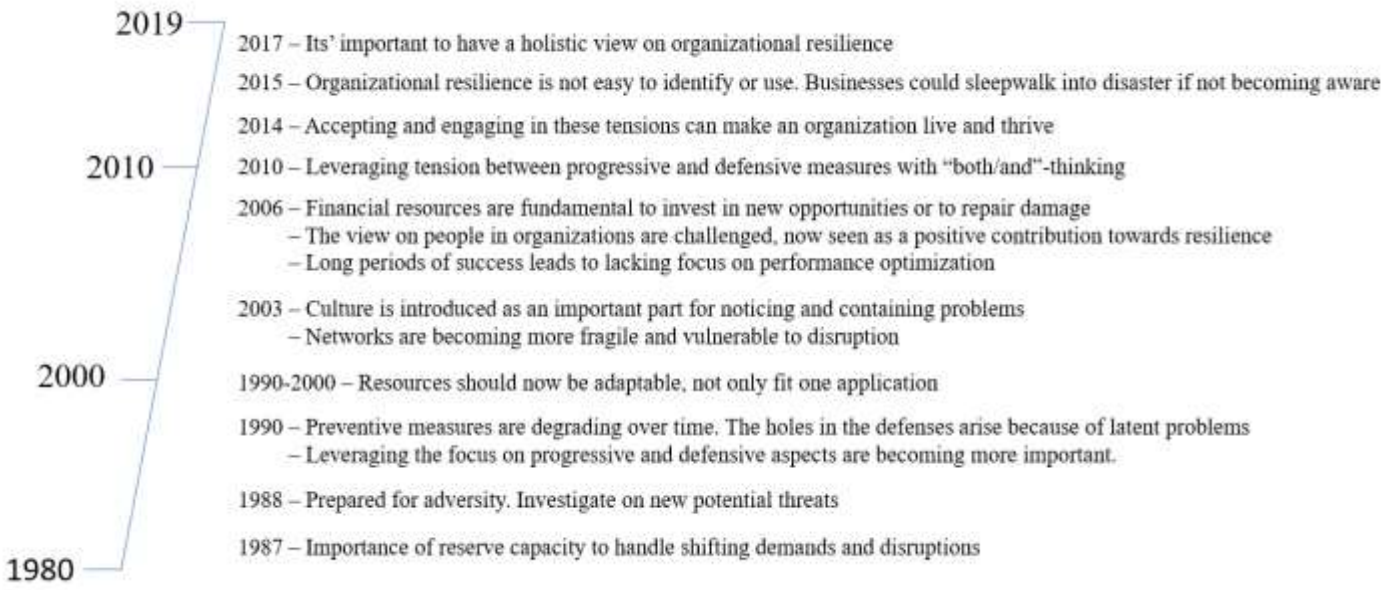

Figure 2.1: Timeline of elements of the term organizational resilience (Denyer, 2017)

One element that seems to be a fundamental part of organizational resilience thinking during the time period from 1987 to 2009, is the focus on the build-up of extra preventive resources (Rochlin, LaPorte and Roberts, 1987; Leveson, Dulac, Marais and Carroll, 2009). Reserve capacity was meant to deal with shifting demands and disruptions in the market. In 1988, Wildavsky (1988) found that to be resilient is the same as being prepared for adversity. This could include investigating potential new threats and act upon them without knowing what's coming. In 1990, Reason (1990) argued that preventive measures are degrading over time. He sees the defensive layers in an organization as a swiss cheese where the holes arise due to problems like lack of maintenance, poor training, personal practice that takes over for written procedures and deviant acts becomes normalized. When the holes in the cheese line up at some point, an incident may occur (Reason, 1990; Snook, 2002).

During the late 1990s and the beginning of 2000, organizational resilience included focus on resources that could be adaptive and then activated when needed. For instance, this could include guidelines for returning to normal operations after an unfortunate event, regardless whether this event being a system failure or a cyber-attack. As challenges arise, the organization can adapt their resources to fit the required measure (Sutcliffe & Vogus, 2003). It seems that the focus evolved from having resources that dealt with defined problems to a more agile, adaptable approach that could fit certain momentary needs and then to reshape when new problems

occurred. Organizational resilience was considered as a way to be flexible and manage crisis in a longer period. However, Hamel and Välikangas (2003) proposed it could also be a source for sustainable competitive advantage. This advantage being elements such as routines for updating software, which is an important factor to reduce the possibility of being hacked.

In 2003 a need for an organizational culture that included the focus on noticing and containing problems was presented (Sutcliffe & Vogus). The view on people in organizations are challenged, not only seeing them as a source of error but also a positive contribution towards resilience (Hollnagel, Woods, & Leveson, 2006). Organizational culture is the main thing distinguishing organizations that quickly recovers after experiencing a disruption from those who falter. Some important aspects thriving organizational culture, are keeping all employees aware and informed on strategic goals, tactical factors and everyday focus elements of the business. Having all employees in the continuous information loop. The power to make decisions given to individuals and teams is also an aspect to be considered. They should be handled the responsibility to take actions on their own when time is critical. They are on site and can respond quickly. Michelman (2007) highlights what he calls “conditioning for disruptions”. What he means by this, is that companies that continually encounters small disruptions are more prepared for disruptions and therefor increase the organizations resilience. Employees in these organizations have more experience and training in handling such situations. The small disruptions become an everyday activity where company’s recover processes are tested continuously. Employees needs to be aware of their responsibility when carrying out their tasks that has been assigned to them, in order for the overall security process in the organization to be successful (Purser, 2004). Employees needs to have clear responsibilities given to them and make sure they understand how to solve their tasks.

In 2006, Gittell, Cameron, Lim, and Rivas addressed that organizations needs to have financial reserves that can be used during times of crisis, acting as an enabling factor to return quickly to full performance. Financial resources are fundamental to invest in new opportunities or repair damage. When organizations enjoy long periods of success without disruptions or failure, they tend to lack focus on performance optimization (Hollnagel et al., 2006). Networks are becoming more fragile and vulnerable to disruption due to the reliance of critical nodes and the pursuit of

gaining efficiency and over-optimization (Christopher & Peck, 2004; Hendricks & Singhal, 2003; Tang, 2006).

Leveraging the focus on progressive and defensive aspects are becoming more important. Leaders needs to address and manage the tension between defensive and progressive views of organizational resilience (Leveson, Dulac, Marais, & Carroll, 2009; Reason, 1990). The leveraging could be done by employing 'both/and' thinking (Farjoun, 2010), which means that actions taken can benefit both defensive and preventive measures. For example; when tackling one problem and the solution could be adapted to other areas afterwards.

Figure 2.2 below summarize the evolution of organizational resilience thinking, by dividing the different views and focus areas into four perspectives; preventive control, mindful action, performance optimization and adaptive innovation. The modern view on resilience includes more of the paradoxical perspective where everything is interconnected with each other. There could be a tendency that organizational resilience thinking is leaning over to supply chain resilience, this because of organizations being interconnected.

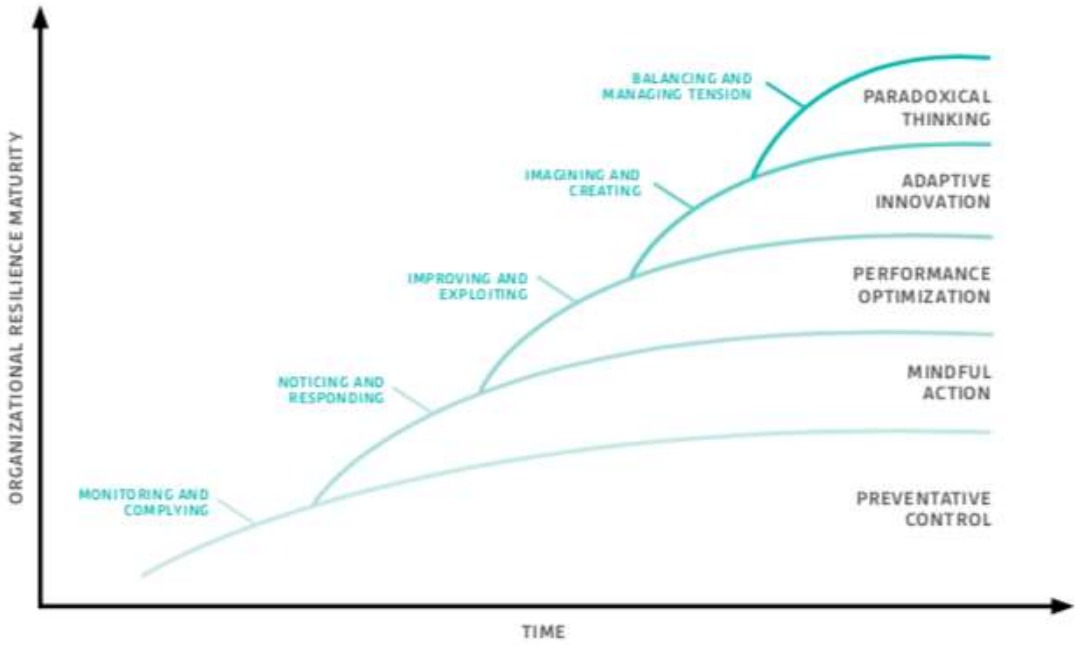

Figure 2.2: The evolution of organizational resilience thinking over time (Denyer, 2017)

Organizational Resilience Today

Many organizational managers refers to organizational resilience as something important to improve, but it seems that there is always something else that becomes more important to address, hence there are many areas in an organization it is important to focus on (Lee, Vargo, & Seville, 2013). Some organizations can even find it challenging to address new entities when they have more than enough with handling their everyday activities. It is also difficult to gain interest from investors and decisionmakers to work on resilience, since it doesn't give a measurable financial return. Organizational resilience is a holistic view and not easy to identify. Therefore, it is understandable that managers who measures everything in finance could lack an understanding of the importance of the topic.

Organizational resilience is not just about bouncing back and returning to normal performance level following a disruptive event. It is also about dealing with both incremental change and sudden disruptions, and to do so in order to survive and prosper (British Standard Institution (BSI), 2014). Howard Kerr , chief executive of the British Standard Institution, understands organizational resilience as something that reaches beyond risk management towards a more holistic view of business health and success. Leflar and Siegel (2013) recognize organizational resilience as a goal, and organizational resilience management as a way to achieve that goal. This is not particularly wrong, although it is also important to keep in mind that organizations can only be more or less resilient, that there is no absolute measure or definite goal (International Organization for Standardization (ISO), 2017).

The ISO 22316:2017 Security and Resilience — Organizational Resilience — Principles and Attributes standard (International Organization for Standardization (ISO), 2017) also emphasizes that there is no single approach to enhance organizational resilience, and that organizational resilience is the result of interaction between attributes and activities. Attributes is in this circumstance considered to be what describes the characteristics of an organization that allow the principles to be adopted, principles that proved the foundation for enhancing an organization's resilience. Activities are guiding the utilization, evaluation and enhancement of these attributes.

One of the attributes mentioned in the latter standard is the development and coordination of disciplines. This is an important attribute as there are many established management disciplines that contribute towards organizational resilience. All management disciplines should be

coordinated so that they individually and collectively contribute to the organization's purpose and the protection of what it values. Relevant management disciplines include risk management, strategic planning, business continuity management, crisis management and supply chain management, to mention a few. It is important to notice that although these disciplines contribute towards organizational resilience, they are insufficient on their own. For instance, business continuity and crisis management have means and objectives to address risks which in turn may result in organizational resilience, but they are not the same thing as organizational resilience (Leflar & Siegel, 2013).

Managers can decide to use resources on organizational resilience, but every employee must be part of the change. According to Välikangas (2010, p. 89), "resilience cannot be commanded". Instead the work on resilience should be a part of the organization's natural activities, becoming and being everyone's responsibility. Välikangas also highlights the importance of trying to turn threats into opportunities and try to do it on daily basis, not only when encountering larger disruptions. This is in accordance with Michelman (2007). By doing so, you train your organization on tackling disruptions better. To make an example, continuous backup of important documentation reduces the impact of server break-down or malfunction. Implementing such measures make resilience becomes an every-day focus and a capability, rather than a concept that only awakes during a disruption (Välikangas, 2010). The British standard BS65000 - Guidance on Organizational Resilience draws on the relationship between all organizational operations and how all plays together to increase its resilience. Figure 2.3 shows this relation.

Figure 2.3: BSI's model for organizational resilience (Kerr, p. 8)

Product excellence, process reliability, and people behavior are essential elements that needs to be present for the organization to become more resilient. Furthermore, to gain resilience there are three functional domains to do so; operational resilience, supply chain resilience and information resilience. By utilizing these functions and achieving higher resilience, there are three key benefits. The organization becomes more strategically adaptable, it gets a more agile leadership and a robust governance. Overall, the work on resilience is a continuous cycle. It must be maintained and implemented as a natural part of the organizational functions to keep its resilience.

Silo Mentality

Silo mentality is used to express organizational behavior where parts of the organization functions are in manner disconnected from the rest of the organization, likewise as grain silos are standalone structures not connected with each other (Cilliers & Greyvenstein, 2012)**.** Organizations could either be so large that communicating with all departments are difficult or it could be the victim of bad communication. According to Willcock (2013), big organizations could be so complex and fragmented that people wanting to interact with the organization are being sent from department to department before finishing their request. The first department does not know what the other department is doing, and it is the customers responsibility to

connect them together by transferring the information. This behavior can be present on an individual-, organizational- and interorganizational level. The departments have often separate roles and they do not need to communicate with each other on a regular basis. Such silo mentality is not beneficial for collaboration and effective communication between departments and/or organizations. According to Dunkel (2009), the cyber-crime problem of today is a direct result of silo mentality in the development of software. He elaborates on the participating parties in the development of software, has different skills and mindsets and that they have different focuses and views on what to include. Their interaction is not well integrated and the communication between them are lacking, hence silo mentality. This setting could also be adapted to employees using the software afterwards, they have different skills and roles and therefore interact and use it in different manners. How they use the software differently, could potentially damage their communication.

For organizations to have effective partnerships with external organizations, it needs to be open, adaptable and flexible. They have to work closer and be more open with each other. Willcock (2013) states that "*a lack of openness leads to a lack of adaptability and the inevitability of stagnation, more radical change or even failure*". Additionally, he presents how organizations can benefit on collaboration when removing the boundaries of silo mentality:

- Understand the business and market context better
- Get an 'outside-in' perspective on the business, such as the voice of the customer
- Examine strengths and weaknesses, opportunities and threats
- Develop the operating framework
- Develop integrated plans
- Have feedback and review processes
- Adapt the plans accordingly

Organizations needs to develop more structured collaboration models to effectively manage tomorrows networked supply chains (Hu & Monahan, 2015). Especially the access to transparent and accurate data is of high importance to be able to address suitable capabilities. Companies that are not willing to be more transparent with each other will decrease their efficiency and robustness. Lack of transparency is often a sign on lack of trust or confidentiality issues. Some

companies have addressed this issue by introducing third party services to handle sensitive information that they are communicating with each other (Hu & Monahan, 2015).

Having a more holistic view of business health and success (Kerr), organizational resilience is about including all levels and departments. It is about abandoning the old approach of managing risk in siloed disciplines to achieve an organization-wide perspective (Leflar & Siegel, 2013). An integrated and multidisciplinary approach will allow organizations to better understand the relationships between risks, identify solutions to problems and to increase the adaptive capacity of the organization to ultimately improve coherence and performance.

2.2 Understanding Organizational Vulnerabilities and Capabilities

Whereas vulnerabilities can be considered *"factors that make an enterprise susceptible to disruptions"*, capabilities are "*attributes that enable an enterprise to anticipate and overcome disruptions"* (Fiksel et al., 2015, p. 81). Välikangas (2010) suggests that vulnerabilities and capabilities can be related to resources available within the organization. Moreover, organizations who are most vulnerable cannot necessary afford the capabilities needed to handle them. This means that organizations that are low on resources such as financial assets or number of employees could be more vulnerable to disruptions, and furthermore, not able to pay for the repairs needed afterwards.

When organizations are becoming more vulnerable, they may be facing unwanted amounts of risks and therefore needs to improve their corresponding capabilities (Fiksel et al., 2015). However, an over investment in capabilities can result in decreased profits. Therefore, it is important to find a balance between investments in capabilities and acceptable levels of exposure to risk. Figure 2.4 illustrates the zone of balanced resilience.

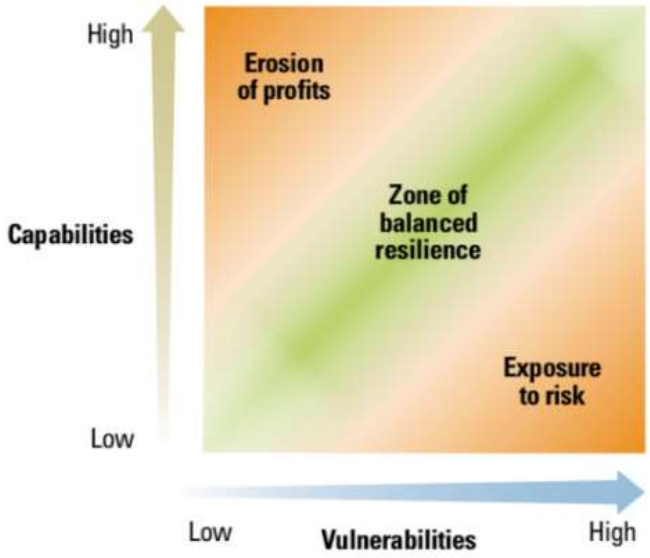

Figure 2.4: The zone of balanced resilience (Fiksel et al., 2015)

2.2.1 Identification and Categorization

Digital vulnerabilities are not always easy to identify, as stated above. This could also have a relation to the lack of literature on this field. There is not much theory on identifying digital vulnerabilities and how organizations can categorize them. However, the theory found is mainly focusing on technical barriers addressing faulty programmed codes or firewall hacking. Following are some examples on how cyber-attacks and cybercrime can be categorized. This will make the foundation for how we chose to categorize the digital vulnerabilities since they are relatable to our study. According to Jouini, Rabai, and Aissa (2014), one way of categorizing them could be by source, agents or motivation. Where is the attack coming from, who are conducting them and what is the motivation behind the attack. Classifying such threats can help the organization to evaluate their impacts and develop strategies to mitigate them (Jouini et al., 2014). When it comes to cyber-security, many articles have divided these into categories. One way of classifying cyber-attacks can be as purpose based, legal based, based on severity of involvement, based on scope or based on network type (Uma & Padmavathi, 2013). While Kumar, Srivastava, and Lazarevic (2006) divides cyber-attacks by impact areas such as networks, operating systems, middleware and electronic payment systems. Gordon and Ford (2006) categorizes cybercrime which includes a human aspect and a technology aspect. If the attack contains mainly technological components it is classified as a type 1. If the attack mainly

consists of high involvement of human factors it is categorized as type 2. Type 1 attacks where mainly from use of software, whilst type 2 where other types that involved a user, for instance; phishing. Jouini et al. (2014) addresses the possible source of the attack as two types: employees' activities or hacker's attack. These examples show different ways of categorizing the theme, it will depend on the context which of them who is most suitable. Levitin and Hausken (2009) addresses the impact from vulnerabilities to be categorized as intentional and unintentional, whereas unintentional is naturally-occurring events or accidents and intentional is attacks from external sources. The categorizations addressed in this sub chapter, are meant to handle technical barriers. In the case of this study these are used as a basis for a new categorization where the humans play a central role instead of the technical equipment. This categorization can be seen in subchapter 4.1.

2.2.2 Digital Vulnerabilities

Digital vulnerability is defined as "*the condition of susceptibility to harm that stems from the use of digital technology*"(Ransbotham, Fichman, Gopal, & Gupta, 2016). The harm can arise from the technology itself, for instance bugs or malfunction in software, external usage of the technology or actions intentionally done by third party to intrude security or privacy by hacking. According to Fitzmaurice (2013) elaborates in his article on "Board Level Security" that people, or employees, are a bigger threat to the digital security than the technology itself. There are more technical breaches in organizations happening from human errors than technical malfunction. It turns out people, the most valuable asset, is also the weakest link in a digital security context. Examples of such vulnerabilities include:

- A miss sent email (a strategy document sent to a competitor)
- Sensitive commercial papers left on a train
- A former employee that was not legally prevented from taking bid information to a competitor
- A laptop left on a plane with password attached
- Careless use of social media giving away intellectual property

Organizations needs to be aware that there is more to cyber-security than only the technical barriers. They need to prepare them self for the new digital age by developing new digital capabilities where organizational goals are aligned with employees and culture, so they are all in

sync (Kiron, Kane, Palmer, Phillips, & Buckley, 2016). *"When people hear cyber-security, they automatically think of IT. So when organizations hear the words cyber-security breach there is often a tendency to leave it with the IT department, not only to deal with the breach but to ensure the breach doesn't happen again*" - Fitzmaurice (2013, p. 28). For the human part, Peltier (2006) also draws on people as an important source of vulnerability, he explains that third parties that want to penetrate organizations can use employees as a way in. By taking advantage of basic human instincts, you can make a way inn to the organization. He calls it social engineering and it consist of utilizing the desire from the employee to be helpful, the tendency to trust people, the fear of getting in trouble and the willingness to cut corners. These are the main reasons for employees to be a vulnerability.

Digitalization means increased visibility, enhanced cloaking, increased interconnectedness and decreased costs (PST, 2019). These new opportunities cause potential for disruption to both individuals and organizations due to vulnerabilities that may not yet fully be understood. In fact, could an increased visibility lead to competitive businesses taking advantage of your endeavor. Attacks on organizations can come from different angles and methods that are being used vary and are under constant evolvement (PST, 2019).

2.3 Capability Thinking and Capability Management

Capabilities can be seen as the organizations skills to achieve their ambiguous goals (Wißotzki, 2018). A capability means to have a competence and ability to do something, it also means to have the right amount of resources who is needed to do something (Sandkuhl & Stirna, 2018a). Resources in this context is for instance money, time, tools and personnel. Capability management is about how to implement capability thinking, its principles and means, for use in the organization. Capabilities help organizations increase productivity and flexibility, and is meant to support organizations handling different challenges related to a dynamically shifting business environment (Sandkuhl & Stirna, 2018a).

Sandkuhl and Stirna (2018b) draws attention to two different ways of applying capability management. The first is a project-oriented use of capability-driven development which means that capability management is only used for clearly identifiable parts of an organization. This could for instance be for certain business services. The other way to apply capability

management is when including the whole organization or certain units with the intention of having a long-term usage.

Capability management is relevant in the context of this thesis, hence organizational resilience is about building a certain set of capabilities to pass the test of time (Denyer, 2017). Digital vulnerabilities can also be mitigated with the right set of capabilities. And finally, organizational resilience is about having a holistic view on the organization as well as with capability management, there is a need for a holistic view of the complex relation between different elements in the organization (Wißotzki, 2018). Capabilities can also be linked to continual improvement, since industries are constantly shifting in terms of innovation and progress, and it is therefore needed to always update the organizations capabilities accordingly (Wißotzki, 2018).

Continual improvement is about identifying potential problems and change the environment to cope with or remove the problem, so its harm doesn't recur (International Organization for Standardization (ISO), 2017). Organizations are built up on individuals that are doing certain processes to accomplish certain goals. These processes are containing different steps that needs to be executed to get the work done, these steps are learned by the individual during experience. However, organizations nowadays ensure that no process lasts forever. Processes that worked well earlier are not necessarily up to date for coming types of work (Hamm, 2016). Therefore, processes that worked well when designed, may not be as efficient today. Continual improvement and constantly changing processes are necessary not to put the organizations survival at risk (Hamm, 2016; X. Huang, Rode, & Schroeder, 2011). The implementation of corrective actions should have a date for completion. After the date of implementation, the organization must reassure that the action taken was effective and working. If the implementation was a success, you strive to find new areas of improvement. If the implementation was a failure, you start over and set a new completion date. In this manner, the organization addresses problems, finds solutions and constantly evaluates them. Hence, PDCA (International Organization for Standardization (ISO), 2017).

The structure of the organization has an effect on continual improvement and learning. A more organic structure has a positive effect on this structure. When the national culture is aligned with the organizational structure, continuous improvement and learning will be effectively fostered.

Organizational group culture can compensate for national culture (X. Huang et al., 2011). It is important to include continual improvement thinking in the organization to stay resilient and competitive. Continual improvement and learning are considered to be one of the most central characteristics of learning organizations (X. Huang et al., 2011) and is essential for the organization to prosper.

3 Methodology

The purpose of this chapter is to present our research strategy and to justify the methodological choices made throughout this thesis. This is important if the study is to be replicated and the same approach and results is desirable. It also allows the reader to gain insight in the research process to be able to evaluate the credibility of the findings on its own. In addition to describing the research design and how the data was gathered and analyzed, we will also include a subchapter that assesses the quality of the research. Prior to this, the context of the study will be presented.

3.1 Research Design

In this study, we were interested in understanding the phenomenon of organizational resilience, and more specifically how it is impacted by digital vulnerabilities. The work of this thesis is derived from a social science perspective. As we were studying a relatively new and rapidly developing field, we found an explorative and phenomenon-driven research approach appropriate. The aim of phenomenon-driven research is to "capture, describe and document, as well as conceptualize, a phenomenon" in order to theorize appropriately and develop research designs (von Krogh, Rossi-Lamastra, & Haefliger, 2012, p. 278). The exploratory nature of this study lead to research questions being proposed instead of hypotheses. These research questions are broadly scoped to give more flexibility and are justified by the phenomenon's importance and the lack of viable theory and empirical evidence (Eisenhardt & Graebner, 2007).

This study would be affected by our personal ontological and epistemological perspectives. Where ontology is considered to be philosophical assumptions about the nature of reality, and epistemology being about the theory of knowledge (Easterby-Smith, Thorpe, & Jackson, 2015). We both believe that there are many "truths" and that facts depend on the viewpoint of the observer, which is in line with a relativistic ontology. On an epistemological level we found ourselves belonging to constructionism. This includes the assumption that there could be many different realities (Easterby-Smith et al., 2015), making it important to gather multiple perspectives through mixed methods and by gathering views and experiences from people with diverse backgrounds. This can be described as triangulation, which will be evaluated in subsection 3.4 about the quality of the research.

Although mixed methods of both quantitative and qualitative methods, are argued to be favorable because of the increased validity and generalizability, does this study apply only qualitative methods. Easterby-Smith et al. (2015, p. 129) informs that "qualitative research tends to be of a more experimental nature and involves open-ended rather than pre-coded questions and responses". Constructionist studies also fits with in the description of qualitative methods as they are based on direct observation and personal contact, and can even take place within a single organization (Easterby-Smith et al., 2015).

Taken into consideration our explorative and phenomenon-driven research approach, our constructionistic epistemology and the lack of existing empirical data, we do believe that a case method with qualitative interviews was suitable. This method is mainly conducted with a deductive approach by moving from a general law to a specific case (Kovács & Spens, 2005), meaning that the theory-driven research questions are guiding the data collection and analysis.

3.2 Data Collection

The process of gathering data in this study started with discovering the interesting subject of organizational resilience. To understand what this concept was about we needed to collect data from a literature review, before we could make research questions that would be answered based on the theoretical framework. Following, where the empirical data collected from the case study by executing qualitative interviews. This data was analyzed and theorized to answer the research questions. When, during the empirical data collection, we did not fully understand certain observations, we returned to theory and performed a new literature review.

3.2.1 Literature Review

Easterby-Smith et al. (2015, p. 13) defines a literature review as "*an analytical summary of an existing body of research in the light of a particular research issue*" where "*researchers describe, evaluate and clarify what is already known about a subject area".* To improve our understanding of organizational resilience and its key issues, concepts and theories, we performed targeted searches through databases and libraries. Search words such as "organizational resilience", "supply chain resilience", "capabilities", "vulnerabilities", "robustness" and so on, was originally typed in the library database Oria and in Google Scholar's

database. These databases gave access to a variety of articles and online books. We also looked at the bibliography in the articles to find additional literature and new search words.

Due to limited time and the fact that literature review was not our primary method of data collection, the review was only vaguely structured and not documented in this study. In similarity to what is described above is the literature review characterized by a snowball effect where one search word and source lead to others.

3.2.2 Case Study

Despite that case methods are dominantly seen as a positivistic research method, is it also consistent with both a relativist and constructionist perspective (Easterby-Smith et al., 2015). According to Yin (2003), a case study as "*an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between the phenomenon and context are not clearly evident*"(2003, p. 13). We found this in alignment with what we want to achieve from this thesis, as opposed to for instance laboratory experiments that isolate the phenomena from their context (Eisenhardt & Graebner, 2007).

Case studies may have different designs depending on what you want to get out from the study. Yin (2003) includes a matrix in his book about case study research that illustrates the basic types of designs for case studies, which is shown in Figure 3.1 below. The matrix is divided into four quadrants depending on whether it is a single-case or a multiple-case design, and whether single- or multiple units of analysis is used. A multiple-case design includes looking at several case studies and is a more positivistic method (Easterby-Smith et al., 2015). This design was regarded as being more robust as the evidence is considered more compelling (Herriott & Firestone, 1983) and typically provide a stronger base for theory building (Yin, 2003). Also Eisenhardt and Graebner (2007) advocates that theory is better grounded, more accurate and generalizable when using multiple-case design.

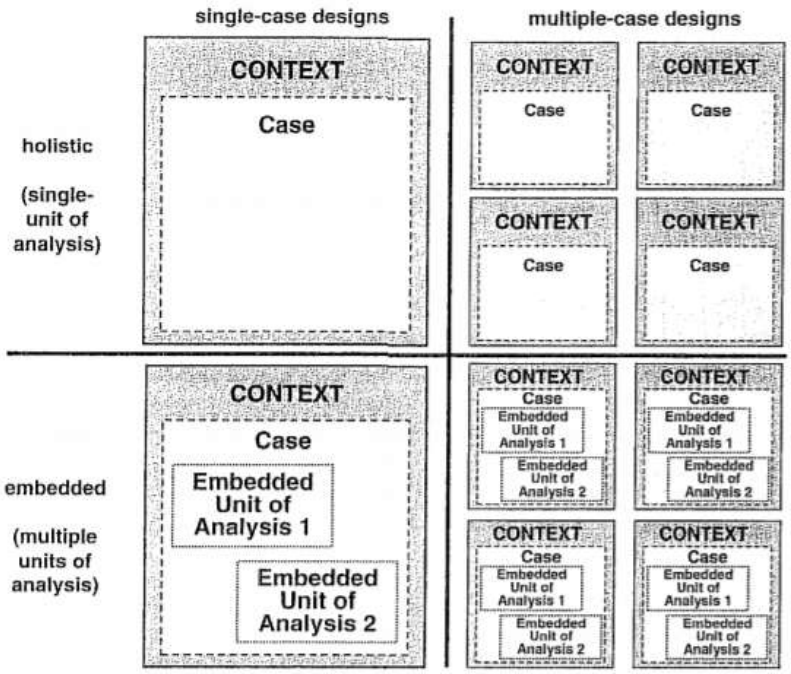

Figure 3.1 : The basic types of designs for case studies (Yin, 2003, p. 40)

Yin (2003, p. 47) states that "*the conduct of a multiple-case study can require extensive resources and time beyond the means of a single student or independent research investigator. Therefore, the decision to undertake multiple-case studies cannot be taken lightly*". This is one of the reasons why we want to maintain a single-case design in this study, but also the fact that rare, critical and revelatory cases are all likely to involve only single cases (Yin, 2003). Eisenhardt and Graebner (2007) refer to Siggelkow (2007) when saying that the existence of a phenomenon can be richly described in single-case design. This rich description was what we seeked to attain from our thesis.

Our single-case study consisted of a four-tiered supply chain, independently investigating each tier. This could be seen as having several small cases within one larger case, making it an embedded single-case study (Easterby-Smith et al., 2015). A holistic view with a single unit of analysis would not have given us the opportunity to investigate the differences between the four tiers, which also arguments for why we chose the embedded approach by having multiple units of analysis. These subunits can "*often add significant opportunities for extensive analysis, enhancing the insights to the single case"* (Yin, 2003, p. 46).

3.2.3 Sampling of Cases and Informants

The sampling in this thesis was performed in a strategic manner, with the purpose of having cases and informants that are relevant to the research questions that are posed. This is coherent with the goal of purposive sampling, which consist of several different approaches (Bryman, 2016). Therefore, we chose representatives from the different tiers that were in a decision-making position. They would also have an overview on their tiers deliverables and able to answer a wide variety of questions related to both the project and their own organization. Our first sampling approach was a stratified purposeful sampling that aimed at illustrating subgroups and by doing so, assisting the progress of comparisons (Miles & Huberman, 1994). We also used a criterion sampling approach were all cases or informants had to meet some criterions, such as those mentioned above, which is useful for quality assurance (Miles & Huberman, 1994).

After constructing our research questions, we looked for a supply chain with several tiers that allows for comparison of different perceptions within the same supply chain, this being a criterion. In particular, the perception of organizational resilience and how it is affected by digital vulnerabilities. Having DNV GL being our facilitator granted us access to a variety of DNV GL's many clients and business partners. Access to both large and smaller companies situated both domestic and foreign, within different industries. Discussions with our DNV GL supervisor about the different opportunities lead us to a project where there were several supply chains that are exposed to digital vulnerabilities in a somewhat higher level than the others were exposed to. The reason why we wanted someone that is highly exposed is because the phenomenon we were looking into is rather new and it is a rapid developing field. For instance, was it less relevant to look at the textile industry compared to IT or developers of artificial intelligence, as they do not have the same level of experience concerning the phenomenon.

By applying the stratified purposeful- and criterion sampling approach, we selected a supply chain providing smaller and supportive industrial IT systems. As mentioned in chapter 0 was this an operational technology that manages industrial processes. Our embedded single-case study implies that we investigate several units of analysis, the units of analysis being each organization in different tiers within the same supply chain. We were given access to the whole supply chain from the operator down to the suppliers, making up four tiers. However, we chose to exclude potential manufacturers and producers of raw material. This exclusion was based on the fact that

we want informants that are extensively exposed to vulnerabilities, and also partly because of the accessibility of certain companies and duration of this thesis. By investigating the four tiers we got different views on the same topic from organizations that were very large, large, medium and small according to number of employees and resources. This is especially interesting to investigate since they all are in the same supply chain and impacts each other regardless of size and position in the supply chain. By receiving different perceptions, we can build theory on how digital vulnerabilities impacts the supply chain when containing widely different organizations and their different perceptions.

When selecting informants within each subcase, we have used the following criteria: 1) being in a position that have frequently communication with the remaining part of the supply chain, and 2) not being in the IT-department or responsible for such business. In the latter criterion, IT is all information technology used for administrative purposes and so on. This is different from the operational technology that is delivered in the project. These criterions were set so that our informants have proper understanding of the supply chain they are a part of, and that they do not work with digital vulnerabilities as solely cyber-security. We didn't want to speak with the expert since they are not representing the general knowledge level of the organization. The informants we were interested in talking to was those that on an everyday basis are exposed to digital vulnerabilities, but do not address these as a part of their job. By talking to these informants would we get information that was not characterized by not knowing anything about the topic, or on the other hand having detailed knowledge about the technical aspects of the phenomena.

Table 3-1 provides a summary of what kind of supply chain we were looking into, what kind of informants we have talked to and to what tier they belong. Regarding sample size was it noticeable that we have only chosen one informant form each of the first three tiers and three informants from the fourth tier. This is due to there only being one operator, one EPC contractor and one system integrator for the operational technology system. Systems suppliers however, are there approximately 20-40 of. With this in mind, we found that choosing three is more representative as there are so many system suppliers compared to operators, contractors and integrators.

Table 3-1: Informants from each organization within the supply chain

"Company"	Supply chain tier	Informant
A large Norwegian operator	1st tier	Contracts Admin
EPC contractor	2nd tier	Engineering Lead (within the system)
System integrator	3rd tier	Integration Manager for projects within the given industry
System supplier	4th tier - A	VP Sales (within the given industry) & Finance Manager
System supplier	4th tier - B	Strategic Account Director
System supplier	4th tier - C	Sales Project Manager

3.2.4 DNV GL and Description of the Case

DNV GL is a consultancy company with competence on cyber-security in addition to many other fields. In relation to this thesis, one or more of the tiers are DNV GL customers. They assist their customers in improving their business in a safe and sustainable manner. DNV GL provides classification, certification, technical risk and reliability analysis along with software, data management and independent expert advice to the maritime sector, the oil and gas sector, and to energy companies. With 80,000 business customers across all industry sectors, DNV GL are also the world leader in the certification of management systems.

The case study is based on a project that is in its last phases, taking place within an industry of great magnitude and importance in Norway. When the project is finished, is it estimated to have cost of approximately 50 billion NOK. The industry has experienced quite a few changes in the past decades, from being characterized by mechanical and manual work to having a higher degree of automatization and being in a digitalization process. Another change is that from focusing tremendously on safety, the industry is now also concerned with environmental consequences and security. As a matter of fact, the operator in the project we investigate have hired dedicated consultants from DNV GL to assist them in their work on cyber-security. This is also how we came to choose this particular case, as DNV GL act as facilitator for this thesis.

Taken into consideration that the industry requires several products and services and that this project is of a considerable size, we naturally had to choose one specific chain of suppliers due to time and capacity limitations. We landed on a supply chain that provides technical devices and systems for communication. These technical devices and systems are advanced and require the use of digital solutions. Several measures and procedures are in place to make sure that these devices and systems are properly secured.

3.2.5 Qualitative Interviews

As previously mentioned, were all information from the case study retrieved by qualitative interviews. According to Eisenhardt and Graebner (2007) are interviews a highly efficient way to gather rich, empirical data, but they do also provoke a "knee-jerk" reaction that the data are biased. This bias is typically linked to both poorly constructed questions and to response bias from the person being interviewed (Yin, 2003). In other words, may interviews be hard to execute in a proper manner, and are also rather time consuming. Mitigating the challenges of performing is best done by having data collection approaches that limits bias (Eisenhardt & Graebner, 2007) and by having proper exercise in dealing with the method. Yet another measure that makes it easier to perform the interviews and at the same time increases the quality, is to be two persons interviewing together. The quality of the research will be further elaborated in subchapter 3.4.

Qualitative interviews could be anything from highly structured to completely open, and even unprepared. While structured interviews help maintaining a direction and progress in the research, more open interviews may enable new insights or theory. In this thesis were semi-structured interviews considered to be preferable, to allow for flexibility (Easterby-Smith et al., 2015) and at the same time make sure we get answers to our research questions. The practical implementation of this method was done by using an interview guide, see Appendix I. This guide divides potential questions for the respondent into categories, with a time estimation per category. A key point here was that the questions only worked as a guide, and that deviations are seen as a positive contribution to the research.

3.3 Data Analysis

Miles and Huberman (1994, p. 10) define analysis as "consisting of three current flows of activity: data reduction, data display and conclusion drawing/verification". Data reduction includes the process of focusing, simplifying, abstracting and transforming the data, with the intension of, among other things, organizing data to allow for conclusions being drawn and verified. A data display permits conclusion drawing and action by providing an organized and compressed assembly of information. An example of designing the data display is when decisions are made about the rows and columns of a matrix for qualitative data. Conclusion drawing and verification consists of deciding what the data means by noting regularities, patterns, explanations and so on, for then to verify it either briefly or with lengthy argumentation. Furthermore does Miles and Huberman (1994) highlight that these three current flows of activity are all a part of the analysis although they occur continuously throughout the life of the research, though the final conclusions may not appear until the data collection is over. The current flows of activity defined by Miles and Huberman (1994) are incorporated in Table 3-2, which gives a description of all the steps in the data analysis that has been performed in this thesis.

In the "joint analysis" step, particularly, did we take advantage of some analytic manipulations presented by Yin (2003, p. 110) originally described and summarized by Miles and Huberman (1994):

- Putting information into different arrays
- Making a matrix of categories and placing the evidence within such categories
- Creating data displays for examining the data
- Tabulating the frequency of different events
- Examining the complexity of such tabulations and their relationships
- Putting information in chronological order using some other temporal scheme

These analytic manipulations were used in a manual analysis, meaning no use of digital or technical tools for analysis. The importance of having set instructions for the data analysis is confirmed by Yin (2003) saying that it is crucial to have analysis approach developed as a part of what he refers to as a case study protocol.

Table 3-2: Description of steps in the data analysis

Step in the data analysis	Description of the step
Case selection	- There was a meeting with DNV GL to investigate different possible cases - The case was chosen on the background of relevance and access.
Data collection from qualitative interviews	- Qualitative interviews of the informants - The interviews were conducted at respective tiers' offices - Both of us being present at each interview
Review of sound records and notes and individual analysis	- Review of the sound records and notes from each of the interviews - While reviewing are each interview individually analyzed
Create a document of temporary findings	- During the latter step, create a document of temporary findings based on the review and individual analysis - Started with one interview together to assure we were consistent
Clarification and correction by the informants	- Sending the temporary findings from each interview to the respective informant - Receive clarifications and corrections by the informants to make sure we understand them correctly
Joint analysis	- After receiving the corrections and clarifications, a joint analysis of all the interviews is conducted - While doing so are the research questions kept in mind
Adding additional information	- If necessary, ask the informants for additional information to further clarify after the joint analysis
Completing the analysis	- After adding the additional information, the analysis is completed

3.4 Quality of Research

When discussing quality of research was it inevitable to include the two terms *reliability* and *validity*. A constructionist asks whether a sufficient number of perspectives is included when evaluating the reliability, while validity is regarding the possibility of similar observations to be reached by other observers (Easterby-Smith et al., 2015). Yin (2003) mentions four tests commonly used to establish the quality of any empirical social research, case studies being one form of such research. The four tests are: *construct validity*, *internal validity*, *external validity* and *reliability*. Internal validity is mainly concerning explanatory studies and is, based on this, not considered in this thesis as it was an exploratory study. Below, in Table 3-3, is a description of the three remaining tests, what tactics can be used for dealing with the tests, and the phase where these tactics occurs.

Table 3-3: Case study tactics, adapted from (Yin, 2003)

Test	Purpose	Case Study Tactic	Phase of research in which tactic occurs
Construct validity	Establishing correct operational measures for the concepts being studied	- Use multiple sources of evidence - Establish chain of evidence - Have key informants review draft case study report	Data collection Data collection Composition
External validity	Establishing the domain to which a study's finds can be generalized	- Use theory in single-case studies - Use replication logic in multiple-case studies	Research design Research design
Reliability	Demonstrating that the operations of a study can be repeated, with the same results	- Use case study protocol - Develop case study database	Data collection Data collection

As the quality of the research increases when these tactics are implemented, have we tried to carry out as many of them as possible. There were however some difficulties, especially regarding external validity and the utilization of purposive sampling. Bryman (2016) states that "because it is a non-probability sampling approach, purposive sampling does not allow the researcher to generalize to a population". As a tactic was theory an important part of our research design, to be able to somewhat "benchmark" our findings. To increase the reliability were there made tactics such as recording the interviews and being two persons interviewing the informants.

Triangulation is another measure that can be taken to increase the quality of the research. Easterby-Smith et al. (2015) describes triangulation as "using different kinds of measures or perspectives in order to increase the confidence in the accuracy of observations". When triangulating methods are multiple perspectives gathered through a mixture of qualitative and quantitative methods. This thesis does not triangulate methods, However, does it triangulate by collecting views and experiences of diverse individuals.

The results of this study can in some extent be generalized to other organizations and supply chain since many other sectors are also experiencing increased. However, specific findings that are purely for either project-based industry or this specific industry, could be of less interest to other parties. Nevertheless, cyber-attacks and human error related to the use of digital equipment would in general be interesting for all types of organizations to learn about.

4 Findings and Discussion

In this chapter we will present our findings and at the same time discuss them in accordance to our research objectives and -questions. The subchapters are a reflection of these research objectives and -questions and are composed in a chronological order, starting with research question one which is divided into two subchapters.

4.1 Key Digital Vulnerabilities

When conducting interviews in our case study, we identified several digital vulnerabilities that impacts the supply chain. These vulnerabilities may be present in the environment that the supply chain operate in, the supply chain itself, or specific organizations within the supply chain. Regardless of where they are present, these vulnerabilities could result in unfortunate events. Unfortunate events that are generated by either intentional or unintentional actions. We consider intentional actions as opportunistic behavior with the intention of harming a supply chain or an organization. Unintentional actions are similar to mis happenings, as a result of being absentminded or having lack of information or experience.

We have categorized the key digital vulnerabilities based on whether the vulnerabilities are related to; the flow of communication- and information, organizational and human elements of software, or formalities and the interpretation of these. Ultimately, are all three categories depending on the organizational culture, and are affected by the fact that the supply chain in this project is temporary.

Communication and Information

Throughout the supply chain is the daily communication mainly happening by e-mail, phone calls and Skype. Face to face meetings are rather rare as Skype and phone calls to a large extent replaces the need for it. However, are the operator, EPC contractor and system integrator (tier 1, 2 and 3) within this project located at the same site, which allow for a wider use of face to face communication. The important thing to remember is that this supply chain consists of only one operator, EPC contractor and system integrator, while there are more than twenty system suppliers. Hence, are e-mail, phone calls and Skype still the main communication channels. The extensive use of e-mail is addressed as the root cause for several digital vulnerabilities.

Firstly, is the large number of e-mail making it harder to detect fake e-mail. Tier 1 states that *"often you have to trust the email being real because the amounts that needs to be answered during a day is enormous".* Phishing-mail and fake invoices is something that all tiers have experienced, but only one tier have made means to reduce this vulnerability. Tier 1 test their employees and project participants with access to their systems by sending unannounced trick-e-mail. If you are fooled more than three times, you must have a conversation with your manager. Also, there is a competition across the departments to see who is the hardest to fool.

A second vulnerability related to the use of e-mail is the possibility of information being sent to the wrong person. Information could possibly be handed to someone with an opportunistic mindset who wants to benefit from it. All tiers recognize that they have either received or sent a misaddressed e-mail. When working at a high speed, could "Anders Hansen" quickly become "Andreas Hansson". This is also something that Fitzmaurice (2013) highlights as a quite ordinary event. We could not observe any preventive actions to reduce this vulnerability. However, does it seem like they send an additional e-mail to the person receiving the misdirected information, making them aware and asking to delete it. If the information is particularly sensitive should a manager be informed.

An even more prevalent vulnerability is having many people on copy when sending e-mail, hereby referred to as CC, which imply that information is unnecessary distributed. It was highlighted by three of the informants that especially one organization within the supply chain tend to have too many people on CC. Tier 4C states that *"it looks like they are adding the whole world. It is incredible how many people that is supposed to be informed"*. Many of the people that is put on CC are employees within the organization, employees that the rest of the supply chain does not necessarily know who is. An issue highlighted by tier 4B, is that you must trust completely strangers with your information.

A good example of trusting strangers was provided by tier 4B, mentioning that health certificates and resumes from all employees going offshore were requested by e-mail from a higher-level tier. The sensitive information was not encrypted or protected in any way, and several unfamiliar persons had been put on CC. When sending sensitive data to one another they trust that the receiving party handles it with respect and confidentiality. Tier 4A had encountered a similar situation where they, in addition to sending the health certificates and resumes, were requested to

send a copy of the passports as well. This is highly sensitive personal information that should be handled with care. It is not easy to be the system supplier and set demands to the operator and EPC contractor on how they should handle this information. Tier 4B explains this by saying "*we do not want to be perceived as difficult*". When sending sensitive data to one another they trust that the receiving party handles it with respect and confidentiality. which could be a disadvantage for the lower-level tiers. There is an unbalance in power and the lower-level tiers are limiting their demands to satisfy the requirements. As well as not wanting to be considered difficult, the lower-level tiers depend on the economical side from their contribution to the project.

The last vulnerability associated with communication by e-mail, is that the information is likely to be kept in the inbox regardless of this information being sensitive or not. This inbox can be accessed from numerous devices, including your smartphone or tablet. Only one of the informants, tier 4C, informed us about limited access to the inbox on devices that were not solely connected to a secured network at the workplace. This vulnerability naturally leads us to use of digital systems for handling information.

Digital Systems for Handling Information

Common for all the organizations is the use of digital cloud services for handling information. The most commonly used service is SharePoint by Microsoft, where departments, project groups or even the entire organization share information with each other. SharePoint is used within each organization and to some extent within the project. Although digital cloud services allow for immediate sharing of information, are some of the tiers concerned with the use of such services. The EPC contractor for instance stated that: "*I'm not really a fan of the cloud service. You know when you put the system in one country, you basically know that the country has access to all the data*". It is considered a vulnerability that the information stored can potentially be viewed by the responsible service provider, and possibly also the government in the country where the server is located.

When it comes to who has got access to the shared information, we found that there is quite a significant difference between the large and the small organizations. In the large organizations, which we consider to be tier 1 – 3, is the information in different folders restricted to a limited

number of people. These people are only allowed access if their work require the information. In the smaller organizations does it seem to be a more open access, where people outside the project also have access to project files. This is justified by the need of access if the responsible person becomes sick or unavailable for some reason. Even though it is practical to grant more people than necessary access, does it create a vulnerability as it is harder to pay attention to who possess critical and sensitive information.

Critical and sensitive information that the operator is responsible for is stored in a separate cloud system. If documentation and specifications are shared from this server will the sender have to send a link to the file rather than the file itself. This ensures that the document does not leave the cloud server, and hence is it not exposed. All receivers must be verified to gain access to the content of the link. The weakness is that the security log-in is mainly a simple username and a password. There is no two-factor authentication or other types of additional barriers.

Software Log-in, Updates and Competencies

We found that security log-in seems to generate vulnerabilities in all the different tiers. Tier 3 express this weakness by saying "*you need an account, but if someone finds my log-in password they can get all information*". Although passwords are being changed every six months, do you only need access once to be able to infiltrate the system. Also is it a vulnerability that "*we use the same login on our systems as on windows*" - tier 4A. In addition to having only one password and username to different types of software, is the software in particular organizations updated on an irregular basis. Some of the organizations run automatic updates when a new version is available, whilst other have the option to postpone their updates. Postponing updates cause a higher risk for attacks, as bugs and weaknesses in the system has not been improved.

Another issue with software addressed by tier 4B is that there are varying competencies regarding the use of different software programs. When collaborating within a supply chain is it preferable to use one common software that all parties understand and feel comfortable with. Varying level of knowledge then lead to simple compromises like sending information by e-mail and storing the information on local servers. The problem we are addressing here is that standard low security programs such as e-mail could pose a threat when handling sensitive information, and moreover does this question the actual use of software programs such as SharePoint.

Formalities and Interpretation

During the tender process are all system suppliers supposed to receive a comply-scheme. This scheme consists of several types of questions including cyber-security, where the answer is whether you comply, partially comply or do not comply. This a way for the operator, EPC contractor and system integrator to check whether the suppliers have the needed requirements or not. The suppliers however, feel to some extent that a variety of the requirements are to extensive and not always possible for them to meet. This is especially true for the smallest suppliers. When the scheme for instance asks if the organization have dedicated personnel that works with cyber-security, the small suppliers have a problem complying. *"We cannot have people in 100% position on these areas"* tier 4A stated, as they do not have the resources to employ that many people, leaving some of the employees to have several responsibilities. Suppliers feel pressured to answer perfectly to even be considered as a supplier. This result in organizations promising more than they can uphold. This is a gray area that is hard to find a solution to. The operator wants qualified and reliable suppliers, but the suppliers have limited resources to be able to fulfill all requirements.

The requirements are written in a very formal manner, making the suppliers hire lawyers to read through them to make sure they understand it right. *"The specifications on cyber-security are written by dedicated people in a department in big companies, the longer down the value chain it gets, the more distant it feels"* said tier 4A, while tier 4C said that *"it is a very formal process"*. These formal requirements, and the distance they create between the top three tiers and the system suppliers, cause digital vulnerabilities as the systems suppliers might not answer completely correct when it comes to cyber-security related questions.

4.1.1 Security Culture in Organizations

Our impression after talking to all the tiers is that the security culture in each organization have a potential for improvement. Even the organizations that appears to have good security measures and guidelines on how to deal with disruptions, do not communicated this well to their operational personnel. Very few of the informants knew much about guidelines or handbooks they can go to if encountering a digital disruption. Tier 4C knew a handbook existed but could not remember what it specifically contained. Tier 3 on the other hand said they had guidelines but that they were outdated, and tier 2 did not know if they had any such things. The most

disturbing response came from tier 4A, who said that if they had a technical problem regarding digital disruptions, they would simply leave it with the guy on IT. The only tier that informed to have distinct routines for their personnel was tier 1, although the informant could not remember straight away what they involved.

Tier 1 was by our impression very security focused and had been attending courses on cyber-security. Also tier 4C had attended such courses, although it was only the informant and a few other key personnel. Nevertheless, did they educate the other employees when coming back from the course. In the other tiers however, did education and training of personnel seem like something that is lacking. One cannot expect the employees on behalf of the organizations to handle disruptions well if they are not trained on handling such events. It is necessary to "condition for disruptions" as Michelman (2007) said. Our findings corresponds with Purser (2004) as we discovered that security awareness-training was not prioritized by most organizations.

Employees do not see themselves as an important part in the organizational puzzle. People are the fundament of all processes and humans makes mistakes, they need to be aware of the potential threat they are posing for the overall resilience (Lacey, 2010). It is important that all levels of employees understand and act upon the policies given in the organization. Digital disruptions are not only affecting IT systems, and working on handling them requires that the whole organization is participating (Denyer, 2017). All it takes to make a breach is one single unaware employee.

4.1.2 Temporary Supply Chain

When asked about what was considered as the most significant digital vulnerability in the project, particularly the supply chain we investigate, tier 1 accentuate the flow of people participating in the project. The informant elaborates that *"I see many people passing through the project that has gained access to selected areas, or even the whole digital system".* The chances of people making changes or manipulating parts of systems or entire systems are eligible. The more people that is involved, the more challenging it is to maintain the overall overview. Tier 2 agreed upon the fact that people can change parameters and corrupt data; *"you can remove the hard disk or other physical equipment, and thereby easily corrupt data"*. The informant added that if someone steal or corrupt a document, their activity will be logged and the

person responsible is uncomplicated to identify. Nonetheless, it is possible and by the time disruption is detected and the responsible is identified the damage might already have been done.

The lower-leveled tiers also found that the temporary nature of the supply chain and the flow of people lead to vulnerabilities. But instead of relating this challenge to access and corrupt actions, did the lower-leveled tiers link the flow of people to communicational challenges. They found it difficult to communicate with someone they had not met, and barely talked to before. Sætre (2009) addresses the ease of communicating with more unknown relations through technology. It is convenient to use technology, and social barriers are broken down. However, does this introduce a vulnerability; you talk to a digital username with a certain mindset, but behind the username is someone completely different.

4.2 Consequences of Ignoring Vulnerabilities

The discussion in this section will be based on the identified key vulnerabilities previously addressed. The consequences of the digital vulnerabilities can be both intentional and unintentional. The intentional consequences such as hacking are mostly those who gets the most attention. Unintentional consequences such as information going astray because of a mis sent email are aspects that are more secretive and maybe taboo to address. It is embarrassing for the person responsible for the action. Therefore, some of the consequences could be hard to address and some are even not heard of.

Receiving fake emails could be damaging to the organization if the employee receiving them intentionally, or unintentionally, follows the guidelines given in the mail. This vulnerability corresponds to Fitzmaurice (2013) findings, and is seen as an example on social engineering (Peltier, 2006). The consequence of being exploited by fake e-mail is that hackers can gain access to the organization's system where the employee now have granted them access. Sensitive information can be unintentionally distributed, and systems can be corrupted. A substantial flow of e-mail makes fake e-mail, a very dangerous element because it is disguised as a real email the employees could receive normally.

The consequence of having many people on CC when communicating via e-mail, is also the increased possibility for sensitive documentation get lost. There are many people receiving the mails and often people that are unknown to the sender. These unknown receivers could

potentially be fake usernames leading to hackers or misspelt addresses leading to third parties not attending the project. Another consequence with many receivers is that people not needing the information has to read the email and make sure it is not of interest. This creates more work and unnecessary activities. There is more information that needs to be processed and this could prevent employees working on other activities. If sensitive documentation such as passports or health certificates are shared with mail, this will definitely cause some trouble with GDPR.

Information is being stored both locally on organizational computers or servers and on cloud services such as SharePoint. The consequence of having single-sign on to the majority of these services and often the same credentials on all of them makes the way for hackers much shorter if they want to exploit the system. "*you need an account, but if someone finds my log-in password they can get all information*" – Tier 3. The level of security is fairly low and having only one single, or few defensive layers is dangerous (Reason, 1990). Less secure platforms make the system more vulnerable and especially unaware employees could be a possible entrance. Another aspect to consider is how easy email is to access from all types of devices. Computers, tablets and cellphones can all be connected to an email account and the level of security on the devices can vary. When all employees have 2-3 devices connected to the system, there will be many devices accessing the system in total. The consequence of this is that there are many access points and possible entrances.

Software updates can be pushed as long as the employee wants in some of the organizations, this comprises a vulnerability since the system has not been updated and may contain bugs that can be exploited. The consequence of lacking security culture where employees are instructed to conduct these updates, is that hackers could gain access to the system through old software which is easier to penetrate than the ones that are updated to cover the latest possible breaches. Together with software updates, password changes can also be postponed for as long as the employee wants in many of the organizations. The consequence of this is that the current password stays for a long time in the system. This gives hackers better time to crack the passcode before it expires and further stay in the system for a longer time period. They could potentially cause tremendous amounts of damage that could be beyond recovery, since they have gained knowledge over time. There can be planted bugs or secret backdoors that can be used at points later.

The level of knowledge regarding the usage of IT-systems in the different organizations could be seen as disproportional. Some are well educated and have good routines on using the systems while others do not. The consequence of having inexperienced and untrained personnel using the systems is that they pose a threat to the overall security because they can be seen as weaker links more likely to be victims of fake email, use of weak passwords and careless handling of sensitive data. There is no point in having great technical barriers if the users of the systems are the main weakness. There is only one weak link needed to exploit a system (Estay & Khan, 2015).

The comply scheme that the suppliers receive at the beginning of the project, must be perceived in a positive manner in order for the supplier to be considered for the project. The consequence of suppliers stating that they have higher competences than they actually have, is undermining the impression of the overall resilience in the supply chain. When asked if the supplier have a dedicated IT-department, and the IT departments actually is only the "IT-guy" could send the wrong signals to the operator. Incidents like this, can cause the operator to think they have the right picture on the level of resilience, while the truth is a lower level. A lower level of resilience will most likely result in vulnerabilities not being discovered, creating a fake image of the actual security state.

The formal writing in the comply scheme is a challenge for some of the suppliers to read. The lawyers they are hiring cost lots of money and work is time consuming. The consequence of the larger tiers sending very specific demands written in an over-technical language is unnecessary usage of resources for the suppliers resulting in less resources on other more important areas, such as cyber-security barriers or training of personnel. Over-technical language can also imply a deviation in the specifications received and the finished product or service delivered since there is a mismatch in knowledge between the operator and supplier.

The larger organization often have dedicated roles to each employee, while the smaller organizations have more than one role for each employee. For instance, the financial director could also be the one responsible for IT and the IT department could in smaller organization just contain one person alone. The consequences of this is that employees could potentially lack the training or knowledge needed to be fully able to address the challenges with for instance cyber-security related issues. This could possibly lead to lower standard in IT-security and/or financial

reports that are not detailed enough. General competence could decrease and therefore cause possible entrances for digital disruptions both with regards to mishaps and hacking.

A low level of knowledge from the employees related to policies or guidelines the organization have, could lead to the organization being paralyzed if encountering a digital disruption. If there is no training on handling such disruptions, organizational recovery could be drastically delayed or even not find place. This can result in huge financial losses, less competitive advantage or even ruining the business.

Lastly, the consequence of having a high flow of personnel in the project leads to less overall control. Furthermore, it leads to an increased possibility of employees or people that have access to systems manipulating or stealing data.

The overall awareness on digital disruptions is in high extent absent, they do not perceive themselves as attractive targets. The consequence of this is that they become sloppy and does not recognize potential threats. This leading to focus on other elements, taking shortcuts or not considering them at all. Not being able to see the potential disruptions present in the work environment is maybe considered to be the biggest and most dangerous consequence of them all. If you are not aware, it will be difficult to build competence in order to mitigate these vulnerabilities.

The consequences of not being aware, maintain focus and build capabilities on handling the mentioned vulnerabilities above, could lead to the company losing its reputation, no longer having a competitive advantage, experience financial losses due to lost sales, crippled systems or loss of critical documentation (Fiksel et al., 2015). Third party receivers of this information could use it to get insight in industrial secrets and become a more attractive organization while yours is failing. Sensitive personal documents can be used for ID-theft or the information could be sold to terrorist groups who wants to benefit on it (PST, 2019). If encountering a cyber-attack, the company's reputation could be damaged, and customers could lose interest in doing business because they are afraid of possible infected products or services.

When finding capabilities, it is important to address the right level of the implementation (Sandkuhl & Stirna, 2018a), and it is important to make sure the right capabilities are developed to the right set of vulnerability. Too strong capabilities could be overprotective and result in

higher expenses and more work (Fiksel et al., 2015). If processes or routines are too difficult to mitigate, the employees could struggle on upholding the organizations defenses.

Some organizations could say it is challenging to include the whole organization in the work of continual improvement and building capabilities. The solution for these organizations could be to implement these activities in certain project-oriented areas. Areas that are clear and identifiable, such as the top management, operational team or logistics department (Sandkuhl & Stirna, 2018a).

When the right set of capabilities are implemented it is important that the organization manages them closely and keeps them up to date, since the operational environment is constantly shifting and the capabilities needs to be both flexible and adaptable (Wißotzki, 2018). You can only be more or less resilient, there is no absolute goal and therefor you need to constantly keep them up to date, processes does not last forever and the capabilities needs to follow the change (Hamm, 2016; International Organization for Standardization (ISO), 2017).

Ultimately, the organizations resilience will be reduced with the consequences mentioned above, it is important, or even as tier 4B stated: “a make or break for organizations”, to address the arising level of digital vulnerabilities. With the right set of capabilities, the organizations can pass the test of time (Denyer, 2017).

4.3 Differences in Perceptions

Digital Vulnerability as a Terminology

When asked about the meaning of the term digital vulnerability, tier 1 answered that it includes two aspects; a physical and a virtual. As an example, the informant mentioned physical securing of servers by using the right type of components to prevent heating and physical access control to the server room. Virtual vulnerabilities, on the other hand, was for instance the possibility to enter the organizations digital networks and systems. Tier 2 understands the term differently and mentions hacking and other types of intrusive actions performed by people that intend to block or stop the system. This also include physical equipment that breaks down as a result of the system being blocked or stopped. A more operational understanding of the term is present in tier 3, where strong engineering is accentuated. The informant states that the system must be built in a redundant way, and that strong design must be imposed by the project. Tier 4A view

organizational resilience and digital vulnerability as coined concepts, and that digital vulnerabilities are present when sensitive information is exposed. This exposure is not necessarily a result of opportunistic intentions, it might as well be the result of a unfortunate incident. One tier that had quite a specific answer was tier 4B, which understands digital vulnerabilities as access delegation, information sharing, firewalls, viruses, DDOS attacks, blackmailing and so on. Tier 4C is more general than tier 4B and consider digital vulnerabilities as hacking into systems where the aim is to make changes or to break down the system.

There are many different perceptions of the term digital vulnerability, only tier 2 and tier 4C shared the same understanding. Repeating the definition by Ransbotham et al. (2016) that digital vulnerability is "*the condition of susceptibility to harm that stems from the use of digital technology",* it becomes clear that almost all the perceptions do not represent actual vulnerabilities. Instead, they represent consequences and capabilities. Consequences of digital vulnerabilities could be hacking and break downs, like tier 2 and tier 4C mentions, and strong engineering and firewalls are capabilities that can reduce the probability of the vulnerabilities. Tier 4A however, recognize exposure of sensitive information as a digital vulnerability, which truly is a vulnerability. It is also noticeable that tier 1 exemplify the physical aspect of digital vulnerabilities by mentioning capabilities, while the virtual aspect is exemplified by the possibility to enter a system which indeed is a vulnerability.

Organizational Resilience as a Terminology

We experienced that the term organizational resilience was rather unfamiliar to all the different tiers. Most of the informants had barely heard about it. Tier 1 understands organizational resilience as "*organizational functions that are to be covered*". Furthermore, does it include challenges directed to the organization being brought forward, as well as designated employees or groups being handed different responsibilities to maintain control over them. The informant from tier 1 associate organizational resilience to the organization's accountability. Being insecure of what the term really include, tier 2 believe it has to do with "*when you keep wanting something*", further describing that you stay resilient by always wanting something. Tier 3 cannot provide an explanation or example of the term organizational resilience, stating that this study was interesting and that they would learn something new. Tier 4A links organizational resilience to GDPR, while tier 4B considered it to include the vulnerable state you are in with

regards to an organization's employees, how it is organized and what processes exist to handle unforeseen events. Tier 4C look at organizational resilience as how a system can be destroyed, "*depending on how things are done in the organization"*. As remarked in the theory, is organizational resilience a holistic view that is not easy to identify. It is therefore to be expected that differences in the perception of the terminology exists. Nonetheless, do all the tiers except tier 3 promote various elements of organizational resilience.

Perceptions and Awareness

An organization's perception of digital vulnerability and organizational resilience cannot solely be based on the perception of the terminology. The level of awareness, based on both direct and indirect statements from the qualitative interviews, should also be considered. We discovered that the biggest difference in perceptions was based on the amount of times the organization had experienced digital threats and unfortunate events. Tier 1 is very aware that being a large operator cause the organization to be an attractive target for opportunistic actions from both inside and outside the organization, and that such actions have occurred in recent time. Being large scale organizations, tier 2 and 3 also experience some of the same actions as tier 1. However, we did sense a form of insecurity from both informants, leading us to believe that the awareness in tier 2 and 3 is not as extensive as it is in tier 1. There is a general belief among the fourth tier that cyber-attacks and other unfortunate events happen, but that it will not happen to them. Tier 4A questions *"why would anybody want our information?"*, while tier 4B do not *"see it as very likely to be targeted"*. Being a bit more hesitant, tier 4C acknowledge that they could be a target but that it is rather unlikely as other organizations are more attractive.

Correspondingly, does it appear that the perceptions present in the first three tiers are quite similar and that the distinction occurs between the third and fourth tier. There are however noticeable differences within the fourth tier that implies that the size of the organization is determinative. Tier 4A, which is the smallest sized system supplier, show tendencies of being less aware than the two other system suppliers, although their understanding of the terminology is more accurate. Tier 4B is somewhat larger in size and more attentive. Their awareness is enhanced by their interest in increasing their capabilities. The largest system supplier, tier 4C, answers vaguely when asking about the two terminologies, but presents a solid awareness based on both the direct and indirect answers during the interview.

None of the informants recognized or acknowledged the statement from NorSIS' report (2018) that Small medium enterprises (SMEs) are a bigger threat to the supply chain than they are aware of. This is a very interesting finding, as there are considerable differences between small and large enterprises when it comes to resources available. However, our findings show that there is a lack of awareness among the smaller organizations, which compromises a vulnerability. It is important to notice that we do not think that SMEs are more vulnerable than other larger enterprises, although we agree with NorSIS' statement that they are a bigger threat than they are aware of.

4.4 Reduced Impact of Digital Vulnerability

All tiers agreed on the importance of addressing their digital vulnerabilities and make suitable capabilities. However, we are afraid the vulnerabilities are hard to identify because of the lack in awareness. Since they have not encountered any serious cyber-attacks it is hard to see the need for capabilities on the field. Nevertheless, regarding the digital vulnerabilities tier 1 hoped to see a focus forward: "*it is extremely important, maybe more important that many of the other things we are doing*". We think the operator has to stand in the front of addressing the issue and make other participating organizations include resilient thinking in their operational environment. "*If not tier 1 have IT-security as a focus, no one longer out in the value chain will have it*" – Tier 4B. The informant continues by saying that tier 1 needs to be clear with tier 2 and guide them on what should be said to the suppliers further down the supply chain: "*It is important how the operator gives guidelines to its suppliers, so that the suppliers give us, the sub suppliers, good guidance. They hold the key for good security work*" – Tier 4B. Since supply chain is a network-based concept, management of risks should be too (Christopher & Peck, 2004). For the organizations to agree on common goals in the project it is important that they receive the necessary information and become able to act upon the expectations they are given. Common goals increase resilience. We suggest that there should be more collaboration in the supply chain on handling digital vulnerabilities. The smaller tiers should help the larger tiers become more progressive and the larger companies can help the smaller ones to include some defensive thinking. Especially collaborating on digital security since it is breaking down the barriers between organizations. The digital vulnerabilities grow every day and new sophisticated methods are being developed continuously. Working on cyber-security and make capabilities on handling

vulnerabilities are something the supply chain agrees on is important to address. "*This becomes more and more important each day*" – tier 4C. Therefore, organizations need to increase their awareness first, because it is hard to build capabilities for something they have not identified and doesn't see as a priority.

Importance of Cyber-Security

The tiers were asked whether they knew any capabilities for mitigating their vulnerabilities. Whereas tier 1 had some routines and focus on it, tier 2, 3 and 4A did not know of any while 4B and 4C also had some guidelines they used. However, they all meant that it was important to address the threat and build capabilities against it. Tier 1 takes this especially seriously "Y*ou can let go working on it, but the day something happens, everyone will ask, what did you do to try to avoid it*" – Tier 1. Our impression is that tier 1 shows a clearer awareness than the rest of the tiers when it comes to the potential threats.

The suppliers needed to comply on certain measures they take to stay cyber-resilient. With the information we learned from tier 4C and 4A, the claims where a little bit heavy on some areas. They also didn't feel that the operator followed up on the claims, it is seen as a very formal thing that is not focused on, or used later. "*They do not follow up on these answers, it is just formal, but use it if there is a breach later on*" - Tier 4A. The operator needs to follow up on the requirements given. For us, it seemed that sending a comply scheme was a traditional thing to do, mostly for covering themselves if something was to happen. It hasn't been followed up earlier and will not now either. Unless there is a breach.

Future Tender Processes

Cyber-attacks do not only hurt business financially, it could also hurt the company's reputation. We asked the project leader and the main contractor whether a supplier, if encountered a cyber-attack, would be chosen again for later projects. Or if they would discard them and never do business again. When doing business with an earlier impacted organization, tier 1 says: "*I will address the theme and ask what happened and what they did with it*". The informant says it is more important that they learned from it and have become more resilient than the attack itself, maybe tier 1 also could learn from their experience. Tier 2 said about their suppliers that "*I do not see the point to remove someone that have been attacked*". Both companies seemed to be

willing to both help and later do business with suppliers that were impacted by an attack earlier as long as they had patched the vulnerability and learned from it. Tier 1 also said that an attack would not give the supplier a worse standpoint in future tender processes: "*Using security measures as a way of excluding organizations is not common, if it is to be used it has to be a very serious weakness*". On a general level, tier 1 says that organizations that takes digital vulnerabilities and organizational resilience seriously, will have a benefit. "*Organizations that focus on organizational resilience and digital vulnerabilities do have an advantage when we are giving projects*". So, one helping tool for suppliers is that they need to focus on the new digital vulnerabilities and how they can both become and stay resilient. This will give them an advantage in future tender processes.

Company Reputation

Companies are afraid of losing business or reputation if they are hit by a cyber-attack. This was a saying we wanted to investigate if was true. Tier 1 and 2 both said that an attack would not mean that they would not want to do business with the company anymore and they were more eager to learn from them than punish them. So, with that said, organizations would not necessarily lose their reputation. However, both tier 4B and C said they would be conscious with going out with the information of being attacked. However, they would tell the other companies they are in business with. So smaller companies are afraid of addressing the subject and be open about it. They would not be as open as Hydro was, and take it to the media, but they would be open to their customers and other possibly affected organizations.

Changes in Large Organizations

Both tier 1 and 2 addressed the issue with being a large organization and the need for being agile and flexible with regards to build capabilities for digital vulnerabilities. They both agreed on that larger organizations never are ahead of development and changes in these organizations often takes longer time to implement since decision-making has to pass through several levels before being implemented. "*Big companies do not move a lot of inertia, it needs to come from the top management*" – Tier 2. And as tier 4B said earlier; vulnerabilities can potentially stay longer in larger organizations since there are more people that needs to be involved. Tier 4C said that there is easier to have a common alignment in a smaller organization than a larger one, there are more

people to handle. "*It is easier for us to think IT-security with fewer employees, the larger organizations have many more employees who needs to think alike*" – tier 4C. Tier 1 seems to be aware of their position but said to us that the informant see themselves they are a little behind and. However, they have an awareness to it which is a good start. Tier 2 said about themselves that they were in the middle of all the decisions made in the project and that it was hard to stay in front of the development of digital capabilities. said this about his organization: "*They are in the middle, big companies are never a head*", which complies to what the other tiers listed here are saying. Larger companies, especially the ones with ownership or high influence in projects, has a responsibility to be more agile and adaptable to change since the suppliers are dependent on them. They also need to be able to communicate the right level of security and capability measures to their suppliers to ensure that the whole supply chain focuses on their own resilience which will affect the overall resilience in the supply chain. Organizations needs to become aware of their responsibility and take actions to cover their part of the overall resilience. One breach in an organization could be affecting the rest of the supply chain.

Increased Focus on Organizational Resilience

All tiers recognized cyber-security as something important, tier 4B even said it is "*make or break*" for companies to address these challenges and develop the right capabilities to withstand disruptions. However, we sense a trend that they have not built capabilities to withstand potential disruptions. Organizations needs to address this issue and ground the elements of organizational resilience deep into their everyday actions. As stated in World Economic Forum (2017), many organizations do not feel that they are equipped with the right tools to manage cyber-risk with the same level of confidence as risk management. This is something we agree on, companies are not familiar with this "new" type of disruption and have not felt the threat. Organizations needs to start seeing them self as vulnerable and take actions to mitigate this vulnerability.

An increased focus on organizational resilience will benefit the organizations to pass the test of time. They need to build new capabilities to be able to mitigate ongoing and common vulnerabilities. Cyber-attacks and opportunistic behavior are becoming more sophisticated every day and there is a need for a constant evolvement in developing capabilities to make sure organizations are not being disrupted. Organizational resilience is a holistic view on all aspects of the organization's entities and actions. The concept is meant to take down silo mentality and

bring the organizations departments closer to each other and make them work as a whole. This is especially important in our digital society where organizations and departments are more accessible to digital disruptions.

5 Conclusion

This thesis contributes to the literature by presenting different perceptions from a four-tiered supply chain. Having employees that on a daily basis communicate with the rest of the supply chain participating as informants, enabled us to investigate how digital vulnerabilities are handled on an operational level. Carefully elaborated guidelines and policies are not valuable when the employees do not understand or know when to make use of them.

The flow of information is happening at a fast pace, and the amount of information communicated is both overwhelming and not necessarily relevant. Information could easily fall into the wrong hands, both by intentional and unintentional actions. Following this, is the extensive use of e-mail considered to be one of the key digital vulnerabilities identified. There are also vulnerabilities originating from a variety of systems with easy access, as well as lack of competencies on how to use applied software. Additionally, we discovered challenges regarding the interpretation of formalities and the distance this create between the tiers. It causes digital vulnerabilities as the systems suppliers might not answer correctly when facing requirements. The consequences of ignoring these digital vulnerabilities could result in a damaged reputation, financial loss or decreased competitive advantage. Ultimately, the key digital vulnerabilities combined with high flow of personnel in a temporary supply chain, leads to an inadequate security culture.

The perception of digital vulnerability and organizational resilience is varying throughout the supply chain. We discovered that the most significant difference in perceptions are based on previous exposure to digital threats and unfortunate events. The main distinction occurs between the third and fourth tier, as the first three tiers actively fear digital threats while the fourth tier hold a denying attitude towards it. Our findings back up NorSIS' report on SMEs being more vulnerable than they are aware of, as the fourth tier is not aware of their position as a possible entry for digital disruptions to infiltrate the larger organizations.

We emphasize a need for organizations to increase their awareness towards digital disruptions. This can be alleviated by implementing resilient thinking in everyday activities, increase collaboration in the supply chain and training personnel. Organizations needs to include the employee's role in the digital environment, not only focusing on the technical barriers. There is a

dominant focus on software, whereas the possibly highest digital vulnerability, the employees itself, are being overlooked. Digital disruptive events can happen to everyone, and there is a need for raised focus on the vulnerabilities causing them. Finally, we accentuate the urgency for more academic literature on the field.

6 References

Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: the concept, a literature review and future directions. *International Journal of Production Research, 49*(18), 5375-5393.

British Standard Institution (BSI). (2014). *Guidance on Organizational Resilience*. (BS65000:2014). BSI Standards Limited

Bryman, A. (2016). *Social research methods* (5th ed. ed.). Oxford: Oxford University Press.

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *The International Journal of Logistics Management, 15*(2), 1-14.

Cilliers, F., & Greyvenstein, H. (2012). The impact of silo mentality on team identity: An organisational case study. *SA Journal of Industrial Psychology, 38*(2), 75-84.

Dalziell, E. P., & McManus, S. T. (2004). *Resilience, Vulnerability, and Adaptive Capacity: Implications for System Performance*. Paper presented at the International Forum for Engineering Decision Making (IFED), Stoos, Switzerland.

Denyer, D. (2017). *Organizational Resilience: A summary of academic evidence, business insights and new thinking*. BSI and Cranfield School of Management

Dunkel, D. (2009). Cyber crime and the integrator: silo thinking's hazardous effects.(Integration Intelligence). *Security Distributing & Marketing, 39*(4), 34.

Easterby-Smith, M., Thorpe, R., & Jackson, P. R. (2015). *Management and business research* (5th ed. ed.). Los Angeles: Sage.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory Building from Cases: Opportunities and Challenges. *The Academy of Management Journal, 50*(1), 25-32.

Estay, D. A. S., & Khan, O. (2015). *Extending supply chain risk and resilience frameworks to manage cyber risk.* Paper presented at the 22nd EurOMA Conference: Operations Management for Sustainable Competitiveness.

Farjoun, M. (2010). Beyond dualism: Stability and change as a duality. *Academy of Management Review, 35*(2), 202-225.

Fiksel, J. (2015). *Resilient by Design : Creating Businesses That Adapt and Flourish in a Changing World*. Washington, DC: Island Press/Center for Resource Economics.

Fiksel, J., Polyviou, M., Croxton, K., & Pettit, T. (2015). From Risk to Resilience: Learning to Deal With Disruption. *MIT Sloan Management Review*.

Fitzmaurice, A. (2013). Board Level Security. *ITNow, 55*(4), 28-29.

Gittell, J. H., Cameron, K., Lim, S., & Rivas, V. (2006). Relationships, layoffs, and organizational resilience: Airline industry responses to September 11. *The Journal of Applied Behavioral Science, 42*(3), 300-329.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2*(1), 13-20.

Hamel, G., & Välikangas, L. (2003). The quest for resilience. *Harvard business review, 81*(9), 52.

Hamm, R. E. (2016). *Continuous Process Improvement in Organizations Large and Small: A Guide for Leaders* (First ed.). New York, New York: Momentum Press.

Harteis, C. (2018). Machines, Change and Work: An Educational View on the Digitalization of Work. In *The Impact of Digitalization in the Workplace* (pp. 1-10): Springer.

Hendricks, K. B., & Singhal, V. R. (2003). The Effect of Supply Chain Glitches on Shareholder Wealth. *Journal of Operations Management, 21*(5), 501-522.

Herriott, R. E., & Firestone, W. A. (1983). Multisite qualitative policy research: Optimizing description and generalizability. *Educational researcher, 12*(2), 14-19.

Holling, C. S. (1973). Resilience and Stability of Ecological Systems. *Annual Review of Ecology Systematics, 4*(1), 1-23.

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience Engineering: Concepts and Precepts*. Hampshire, England: Ashgate Publishing, Ltd.

Hovland, K. M. (2019). Cyberangrep koster opptil 450 millioner. *e24*. Retrieved from https://e24.no/boers-og-finans/norsk-hydro/cyberangrep-har-kostet-hydro-opptil-450-millioner/24612353

Hu, M., & Monahan, S. T. (2015). Sharing supply chain data in the digital era.(Supply Chains). *MIT Sloan Management Review, 57*(1), 96.

Huang, K., Siegel, M., & Stuart, M. (2018). Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys, 51*(4), 70.

Huang, X., Rode, J. C., & Schroeder, R. G. (2011). Organizational structure and continuous improvement and learning: Moderating effects of cultural endorsement of participative leadership. *Journal of International Business Studies, 42*(9), 1103-1120.

International Organization for Standardization (ISO). (2017). *Security and Resilience —Organizational Resilience — Principles and Attributes*. (ISO 22316:2017). Geneva: ISO

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science, 32*, 489-496.

Kerr, H. *Organizational resilience: Harnessing experience, embracing opportunity*. United Kingdom: BSI

Khan, O., & Estay, D. A. S. (2015). Supply chain cyber-resilience: Creating an agenda for future research. *Technology Innovation Management Review*(April), 6-12.

Kiron, D., Kane, G. C., Palmer, D., Phillips, A. N., & Buckley, N. (2016). Aligning the organization for its digital future. *MIT Sloan Management Review, 58*(1).

Kovács, G., & Spens, K. M. (2005). Abductive reasoning in logistics research. *International Journal of Physical Distribution & Logistics Management, 35*(2), 132-144.

Kumar, V., Srivastava, J., & Lazarevic, A. (2006). *Managing cyber threats: issues, approaches, and challenges* (Vol. 5): Springer Science & Business Media.

Kunreuther, H. (2006). Risk and reaction. *Harvard International Review, 28*(3), 37-42.

Lacey, D. (2010). Understanding and Transforming Organizational Security Culture. *Information Management & Computer Security, 18*(1), 4-13.

Lee, A. V., Vargo, J., & Seville, E. (2013). Developing a tool to measure and compare organizations' resilience. *Natural Hazards Review, 14*(1), 29-41.

Leflar, J. J., & Siegel, M. H. (2013). *Organizational resilience : managing the risks of disruptive events : a practitioner's guide*. Boca Raton: CRC Press.

Leveson, N., Dulac, N., Marais, K., & Carroll, J. (2009). Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems. *Organization studies, 30*(2-3), 227-249.

Levitin, G., & Hausken, K. (2009). Redundancy vs. protection in defending parallel systems against unintentional and intentional impacts. *IEEE transactions on reliability, 58*(4), 679-690.

Meyer, A. D. (1982). Adapting to Environmental Jolts. *Administrative science quarterly, 27*(4), 515-537.

Michelman, P. (2007). Building a Resilient Supply Chain. *Harward Business Review.* Retrieved from https://hbr.org/2007/08/building-a-resilient-supply-ch

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis : an expanded sourcebook* (Second ed.). Thousand Oaks, Calif: Sage.

Morgan, S. (2016). Hackerpocalypse: A Cybercrime Revelation. Retrieved from https://cybersecurityventures.com/hackerpocalypse-original-cybercrime-report-2016/?fbclid=IwAR0NsWPZf-DBsOVoSHiJr3xR74M9q9m1_SfFT4bwCBpYFVTRsrGws0gDEqw

Peltier, T. R. (2006). Social Engineering: Concepts and Solutions. *EDPACS, 33*(8), 1-13.

Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *The International Journal of Logistics Management*, 124-143.

PST. (2019). *Trusselvurdering 2019*. Retrieved from https://pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf

Purser, S. (2004). *A Practical Guide to Managing Information Security*. Norwood: Artech House.

Ramanathan, U. (2014). Performance of supply chain collaboration–A simulation study. *Expert Systems with Applications, 41*(1), 210-220.

Ransbotham, S., Fichman, R. G., Gopal, R., & Gupta, A. (2016). Special Section Introduction—Ubiquitous IT and Digital Vulnerabilities. *Information Systems Research, 27*(4), 834-847.

Reason, J. (1990). *Human Error*. Cambridge: Cambridge University Press.

Sandkuhl, K., & Stirna, J. (2018a). *Capability Management in Digital Enterprises*.

Sandkuhl, K., & Stirna, J. (2018b). *Organizational Adoption of Capability Management*.

Sheffi, Y. (2005). *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*. Cambridge, Massachusetts: MIT Press.

Sheffi, Y., & Rice, J. B., Jr. (2005). A supply chain view of the resilient enterprise: an organization's ability to recover from disruption quickly can be improved by building redundancy and flexibility into its supply chain. While investing in redundancy represents a pure cost increase, investing in flexibility yields many additional benefits for day-to-day operations. *MIT Sloan Management Review, 47*(1), 41.

Siggelkow, N. (2007). Persuasion with case studies. *Academy of Management Journal, 50*(1), 20-24.

Snook, S. A. (2002). *Friendly fire: The accidental shootdown of US Black Hawks over northern Iraq*: Princeton university press.

Sutcliffe, K. M., & Vogus, T. J. (2003). Organizing for Resilience. *Positive Organizational Scholarship: Foundations of a New Discipline, 94*, 110.

Sætre, A. S. (2009). *Kommunikasjon i organisasjoner : perspektiver og prosesser*. Bergen: Fagbokforlaget.

Tang, C. S. (2006). Robust Strategies for Mitigating Supply Chain Disruptions. *International Journal of Logistics: Research Applications, 9*(1), 33-45.

The Norwegian Center for Information Security (NorSIS). (2018). *Trusler og Trender 2018-2019*. NorSIS Retrieved from https://norsis.no/trusler-og-trender-2018-1019/

Uma, M., & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and their Classification. *IJ Network Security, 15*(5), 390-396.

van der Vegt, G. S., Essens, P., Wahlström, M., George, G., & Som, O. B. (2015). Managing risk and resilience. *Academy of Management Journal, 58*(4), 971-980.

von Krogh, G., Rossi-Lamastra, C., & Haefliger, S. (2012). Phenomenon-based Research in Management and Organisation Science: When is it Rigorous and Does it Matter? *Long Range Planning, 45*(4), 277-298.

Välikangas, L. (2010). *The Resilient Organization: How Adaptive Cultures Thrive Even When Strategy Fails*. United States of America: McGraw-Hill Companies, Inc. .

Willcock, D. I. (2013). *Collaborating for Results: Silo Working and Relationships that Work*. Farnham, Surrey: Ashgate Publishing Ltd.

Wißotzki, M. (2018). *Capability Management Guide: Method Support for Enterprise Architectures Management*. Wiesbaden: Wiesbaden: Springer Fachmedien Wiesbaden.

World Economic Forum. (2017). *Advancing Cyber Resilience Principles and Tools for Boards*. Retrieved from http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf

Yin, R. K. (2003). *Case Study Research: Design and Methods* (3rd ed. Vol. 5). Thousand Oaks, Califfornia: Sage.

UNIVERSITY OF AGDER

Appendix I

Interview guide

"Digital vulnerabilities impact on organizational resilience:

A case study of a supply chain's different perceptions"

Phase 1: **Framework**	**1. Casual talk (5 min)** - Informal talk where the thesis is explained and put into context
	2. Information (5 min) - Describe the purpose of the interview - Inform about how the audio recording of the interview is stored locally on the recorder, not connected to the internet, and that it is deleted after submission of the paper - Inform about how information is stored on the University of Agder's OneDrive and that the retention of information is applied for and approved by the NSD (Norwegian Centre for Research Data) - Inform about anonymization of the interviewee - Clarify the need for confidentiality - Ask if anything is unclear and if the interviewee have any questions
Phase 2: **Experiences**	**3. Transition questions: (10 min)** - Clarify the organizations delivery to/ participation in the Martin Linge project and the interviewee's area of responsibility - Clarify the interviewee's knowledge of key concepts such as organizational resilience and digital vulnerability
Phase 3: **Focus area**	**4. Key questions: (30-40 min)** <u>Digital vulnerability</u> - Determine how the communication takes place - Clarify the digital processing of information - Get an insight into how digital control systems are used - Clarify which internal processes and external requirements exist to avoid that vulnerabilities are unknown, misjudged, not understood or inadequately communicated

	Organizational resilience This section considers organizational resilience related to digital vulnerability, in contrast to for instance financial or operational vulnerabilities. - Define vulnerable and resilient areas - Retrieve an overall view of the use of resources related to increased resilience within the organization - Identify the internal approach used to achieve increased robustness
	Supply chain - Get a description of how internal and external security requirements are interpreted and communicated between customers and suppliers - Understand how vulnerabilities are dealt with in the supply chain - Obtain information about the experienced focus on resilience in the supply chain
Phase 4: **Review**	**5. Summary (10 min)** - Discuss the interviewee's view of resilience as a focus area going forward - Summarize the immediate observations and get a confirmation that we have understood the interviewee correctly - Inform that information from the interview will be sent afterwards for the interviewee to look through, and that objections are welcome if there are misunderstandings or if it is desirable to add information