

Who hacked my toaster?

– A study about security management of the
Internet of Things

Vem har hackat min brödrost?

– *en studie om säkerhetshantering av*
Internet of Things

Mårten Hakkestad
Simon Rynningsjö

Supervisor: Jonathan Crusoe
Examiner: Malin Granath

Abstract

The Internet of Things is a growing area with growing security concerns, new threat emerge almost everyday. Keeping up to date, monitor the network and devices and responding to compromised devices and networks are a hard and complex matters.

This bachelor's thesis aims to discover how a IT-company can work with security management within the Internet of Things, this is done by looking into how a IT-company can work with updating, monitoring and responding within the Internet of Things, as well what challenges there are with working with this.

A qualitative research approach was used for this case study along with an interpretative perspective, as well as abductive reasoning. Interviews were performed with employees of a large IT-company based in Sweden, along with extensive document analysis.

Our bachelor's thesis results in challenges with Security Management within the areas updating, monitoring and responding along with how our Case Company works with these security challenges. Largely these challenges can be summarized that everything is harder with the number of devices there are within the Internet of Things

Keywords: Internet of Things, IoT, Updating, Monitoring, Responding, Security Management, Cyber Resilience, Middle of Life, MoL

Sammanfattning

Internet of Things eller Sakernas internet är ett växande område med en växande hotbild och nya hot uppkommer dagligen. Att hålla sig uppdaterad, övervaka nätverk och enheter samt att reagera på att enheter och nätverk blir hackade är en svår och komplicerad uppgift.

Den här uppsatsen ämnar undersöka hur ett IT-företag kan arbeta med säkerhetshantering inom Internet of Things. Detta har gjorts genom att kolla utmaningar och säkerhetslösningar inom de tre områdena uppdatera, övervaka och reagera.

En kvalitativ forskningsmetod har använts i denna fallstudie tillsammans med ett tolkande synsätt och en abduktiv ansats. Vi har utfört intervjuer på ett stort IT-företag baserat i Sverige tillsammans med en utförlig dokumentanalys.

Resultatet av denna uppsats påvisar ett antal utmaningar inom säkerhetshanteringen inom områdena uppdatera, övervaka och reagera tillsammans med hur vårt fallföretag jobbar med att motarbeta dessa utmaningar. I stort sett kan utmaningarna sammanfattas till att allting är svårare när mängden enheten är så hög som den är inom Internet of Things.

Nyckelord: Sakernas Internet, Internet of Things, IoT, Uppdatera, Övervaka, Reagera, Säkerhetshantering, Cyber Motståndskraft, Cyber Resilience, Mitten av Livet, MaL

Table of contents

1 Introduction	5
1.1 Background	5
1.2 Problem	6
1.3 Purpose	8
1.4 Research Questions	8
1.5 Delimitation	8
1.6 Target Audience	9
1.7 Disposition	9
2 Methods	10
2.1 Research Approach	10
2.2 Research Process	11
2.3 Case Studies	11
2.4 Finding Literature	12
2.5 Document Analysis	12
2.5.1 White papers	13
2.5.2 Website	14
2.6 Semi-structured Interviews	14
2.6.1 Performing interviews	15
2.6.2 Transcribing Interviews	15
2.6.3 Snowball sampling	16
2.7 Email interview	16
2.8 Analysis Method	17
2.9 Reliability, Validity and Ethics	17
3 Theory	18
3.1 Internet of Things	18
3.2 Organization	19
3.3 Digital Security	20
3.3.1 CIA Triad	20
3.3.2 Cyber Resilience	20
3.4 Product Lifecycle Management	22
3.5 Security Management	23
3.5.1 Monitoring	23
3.5.2 Updating	24
3.5.3 Responding	24
3.6 Previous Research	25
3.6.1 Hej hopp	25

3.6.2 Large Number of Different Devices	25
3.6.3 The Pillars of Security	26
3.6.4 Technical Solutions vs Human Training	26
4 Empirical Findings	27
4.1 The Case Company	27
4.1.1 Respondents	27
4.1.2 White Papers	28
4.1.3 Website	29
4.2 Updating, Monitoring, and Responding	31
4.2.1 Updating	31
4.2.2 Monitoring	32
4.2.3 Responding	34
4.3 Challenges with IoT Security Management	35
5 Analysis	38
5.1 Updating	38
5.2 Monitoring	40
5.3 Responding	41
5.4 The Three Areas Intertwined	42
5.5 Challenges with IoT Security Management	42
5.6 Analysis Summary	45
6 Conclusion	45
6.1 Restating Purpose and Research Questions	46
6.2 Updating	46
6.3 Monitoring	47
6.4 Responding	47
6.5 Challenges with IoT Security Management	48
6.6 Our Contribution	49
7 Reflection	49
7.1 Reflection	49
7.2 Future Research	50
8 Reference List	52
8.1 General references	52
8.2 Case references	55

1 Introduction

1.1 Background

Imagine waking up one night to a strange voice emanating from your baby monitor. On top of that, it is screaming obscenities at you and your child. This is one consequence of when *Internet of Things* (IoT), an umbrella term for all connected devices, lack security, writes Albrecht and McIntyre (2015) in an opinion piece in *IEEE Technology and Society Magazine*. But why are these devices getting hacked? Is it because of a lack of security or a greater underlying issue?

IoT devices have a life expectancy of 10 to 20 years and despite this, they get very few software updates during their lifetime (van Oorschot, 2018). This poses a major security risk for IoT systems. Van Oorschot (2018) writes that a goal with IoT is to be able to read and control the physical world through devices in what he calls a Cyber-physical system. These are systems that operate in, and alter, both the physical world and the internet. These systems, he explains, can contain everything from infrastructure, such as electricity grids and water supply, to home electronics, such as mobile phones, electronic door locks, and health monitors. If something goes wrong in such a system, due, for example, to configuration errors, mismanagement, or errors during operation, that fault can have an impact on the physical world. It is easy to see how much damage could occur if the connected infrastructure were to be compromised, potentially leaving people without water or electricity. Van Oorschot (2018) also writes that the majority of all devices are connected to IoT systems wirelessly which creates a greater demand for security management of these devices than wired devices. He continues that this is not something new, however, stating that the scale of which this is happening is new as there is an increasing number of connected devices. He explains further that it can be considered reasonable to expect everyday users, and, especially, those with limited technical knowledge, to have trouble with managing a larger number of connected devices. He explains that the problems that can occur because of poor management of these devices has already been shown, referring to the Mirai botnet attack mentioned earlier.

A prerequisite in IoT is that there are a lot of devices that need to have very low energy consumption. This is due to the need to be able to operate for a long time without getting any power recharge (Andrea, Chrysostomou, & Hadjichristofi, 2015). This period, they explain, can be as long as multiple years. Because of this requirement of low power consumption and the limited processing power of these devices, they cannot run complex encryption algorithms to make sure others cannot modify or read their data. This issue is also acknowledged by

Sadeeq, Zeebaree, Qashi, Ahmed, and Jacksi (2018), who also explain that a challenging part of implementing security in these devices is finding a lightweight and fast enough algorithm with a high enough level of security to be able to run with these limitations.

One underlying challenge with IoT is that there is no agreed-upon architecture for building connected systems (Yakimenko, Belov, Goncharuk, & Stubarev, 2018). Different devices in your home can have different encryption methods, wireless protocols, and even different technology for wireless connections like Wi-Fi or Bluetooth. The technical bridges needed to make sure all these differences in devices can operate together will thus multiply fast. Yakimenko, Belov, Goncharuk, and Stubarev (2018) explain that even if the systems are secure by themselves when thrown together it results in a network that is only as strong as the weakest link.

Another challenge that we see is that security management for the Middle of Life of IoT devices is a hard and complex matter which leads to weaker security within the IoT. The product life cycle is the whole life cycle of a device, from development to when it is deprovisioned. The Middle of Life is the time period between when the device has been delivered and set up until it is taken down. Soós, Kozma, Janky, and Varga (2018) mention that there are several models for the product life cycle of devices, but that their foundation is very similar. We have chosen the model defined by Soós, Kozma, Janky, and Varga (2018) because it is to us the clearest and easiest to understand of the different models.

Soós, Kozma, Janky, and Varga (2018) write that Product lifecycle management (PLM) helps companies to collect valuable information from their devices during its product lifecycle. This information can have a significant and positive impact on the success of the company's processes if it is utilized. They write that PLM consists of three stages. The Beginning of Life (BoL) stage regards the designing and development of the products, the Middle of Life (MoL) stage which concerns configuration, updating, maintenance and monitoring of the products, and End of Life (EoL) stage which concerns de-provisioning and retiring of products.

A concept within security management is Cyber Resilience it is described by Aoyama, Naruoka, Koshijima, Machii, and Seki (2015) as the ability of organizations to deal with cyber-attacks. Cyber resilience as a concept focus on that organizations need to reduce the impact of cyber-attacks and quickly respond, adapt and learn from them. De Crespigny (2012) writes that cyber resilience is a requirement for organizations and that disconnecting organizations from the internet is not a viable option any more due to the opportunities the internet brings to organisations.

This leads us to the three problem areas: *monitoring*, *updating* and *responding*. *Monitoring* is the process of ensuring that only legitimate devices have access to the network and other devices, that all software updates are authentic, and that only authorized people can access their data (Miettinen, van Oorschot, & Sadeghi, 2018). *Updating* is the process of updating already delivered devices with new security measures or bug fixes. *Responding* is the process of responding to compromised devices.

1.2 Problem

It is not only your baby monitors on the line, but indeed also your toaster, your fridge or even your toothbrush. These IoT devices are often hacked with the intent to be made into bots in a botnet, a group of devices hacked with malicious software that are controlled as a group with malevolent intent, one famous example is the Mirai botnet (Kolias, Kambourakis, Stavrou, & Voas, 2017). Van Oorschot (2018) explains that botnets are often used to perform disruptive attacks against many different targets, with the goal of making them unavailable for use, leading to companies losing money due to the botnets making vital devices or services, such as hospitals and banks, unavailable for use. Symantec (2019), a security company that annually releases an internet security threat report about the latest trends in cybersecurity attack, which states that botnet viruses were the biggest IoT threat in 2018. In their 2018 report the company showed an increase of 600% in the number of attacks against IoT devices between 2016 and 2017 (Symantec, 2018). Furthermore, these numbers have not significantly changed in the report from 2018, showing only a 0.2% decrease from the previous year, proving that the trend is ongoing for now (Symantec, 2019).

Not only are your IoT devices at home at risk of being hacked, but infrastructure using IoT devices is also vulnerable, both of disruptive attacks and of being hacked itself. One example of this happened in December 2015, where hackers crashed a power grid in Ukraine and about 230 000 citizens were without power for hours (Greenberg, 2017). This event did not cause too much damage, the power was restored quite quickly and no one was hurt. Although this event leaves a dangerous precedent and leaves us wondering if it can take down the power grid for good. The virus that took down the power grid had the ability to seek out IoT devices in the network, thus spreading the virus further (ibid.). In September 2018 (BBC, 2018), ransomware hackers hacked IoT devices, such as the departures and arrivals screens in Bristol airport, leading to delays and issues for travelers going through the airport as the employees had to resort to handwritten departures and arrivals screens.

According to a study done by Statista (2016), there are going to be seventy-five billion connected devices worldwide by the year 2025 compared to the twenty-six billion today. These billions of interconnected devices are what together make up the IoT. The collection of

all internet-connected devices is called the IoT and is based on the assumption that someday everything might have a computer in it and be connected to the internet (ITU, 2005). The IoT has grown organically over the course of its lifetime, as opposed to being engineered and developed into being from the beginning. Companies and hobbyist have developed devices individually and connected them to the internet at an unprecedented speed. The need has now arisen to work with IoT as a whole instead of on a unit or device level, as the security threats endanger IoT as a whole.

As mentioned earlier there are a lot of things that can go wrong when more and more devices are connected with potentially terrible outcomes on both an individual level and a societal level. Regarding the technical limitations and lacking device management how can companies operate to keep their networks of IoT devices secure? This is what we intend to answer in this bachelor's thesis.

1.3 Purpose

The purpose of this bachelor's thesis is to study how a large IT-company can work with product safety management during the Middle of Life of the Product Life Cycle for IoT devices with a focus on the three areas updating, monitoring and responding. This will then be compared to theory and previous research.

Our bachelor's thesis results in insight into how an organization works with IoT MoL Security Management contrary to how it should be done according to theory and previous research. We will look more into priorities, policies, and guidelines more than actual processes in how it is done in the organization compared to processes according to theory.

1.4 Research Questions

- How can a large IT-company work with updating, monitoring and responding for IoT Security Management?
- What are the challenges of working with IoT Security Management?

1.5 Delimitation

For this bachelor's thesis, we only looked at how an IT-company can ensure product safety during the Middle of Life of the Product Life Cycle. We have not looked at security measures the customers themselves can manage. While a study on the the whole lifecycle or the technical aspects would have been interesting it does not fit within the scope of our bachelor's thesis. Empirical data for our bachelor's thesis has been created on a large IT-company based

in Sweden actively working within the IoT sphere which will limit the possibility to generalize our result to companies of similar size and prerequisites.

1.6 Target Audience

The target audience for this bachelor's thesis is scholars and other students. Mainly scholars and students within computer and organizational research, also known as information systems. It is also aimed at suppliers of IoT services, especially suppliers that work with Middle of Life Security Management.

1.7 Disposition

Introduction

An introduction to the subject of security management of Middle of Life in IoT devices. Our purpose and research questions are stated here.

Methods

An explanation of why we have chosen a qualitative approach, interpretive perspective, and abductive reasoning, as well as why we have chosen to use semi-structured interviews, document analysis. Lastly, we explain how we will use sorting and reducing as the analysis method.

Theory

An overview of previous research and theory relevant to this bachelor's thesis. A description of the concepts of the internet of things, the CIA triad, cyber resilience, and product lifecycle management. We provide an overview of the areas of monitoring, updating, and responding, some previous research on the field of the bachelor's thesis, and describes the difference between technical solutions vs. human training.

Empirical findings

Gives a brief description of the case, the interviewees and the documents we analyzed. The findings are presented in the areas of updating, monitoring, responding, and challenges with IoT security management, for example why more automation is needed but also hard to implement.

Analysis

Describes the correlations and differences we have seen between the literature and empirical data. The analysis is presented again in the areas of updating, monitoring, responding, and

challenges with IoT security management. It is for example described that the number of devices is one of the core issues in IoT management.

Conclusion

In the conclusion we restate the purpose of our bachelor's thesis and our research questions. The areas of updating, monitoring, responding, and challenges with IoT security management are used to present our conclusions and includes, inter alia, that responding to attacks and threats against IoT require both human agents and automated systems.

Reflection

A reflection of what this bachelor's thesis has accomplished, some weaknesses and strengths with our bachelor's thesis, as well as an insight into what future research can be done in the field.

2 Methods

In this part, we will explain the qualitative methods used to gather and analyze data for the bachelor's thesis. We will describe why we have used a qualitative method, abductive approach and an interpretive perspective for this bachelor's thesis.

2.1 Research Approach

We chose a qualitative research approach to fulfill the purpose of this bachelor's thesis. Qualitative methods allow us to go deeper into and understand our research. It allows us to actually understand how our respondents experience. By using qualitative methods, the research is able to give insight into people and how the experience reality. We believe this is what was needed to get the information that we need to answer the research questions, as we are looking into how it is to work with IoT security management as an organization.

The interpretive perspective was used for this bachelor's thesis. The perspective works under the assumption that access to reality is not objectively given but through social constructions, through people and their experiences (Myers, 1997). We will look at how a company works with IoT security, and how they experience working with it, which is a subjective matter since it will not be the objective answer of to how to work with IoT security, as other companies may do it differently and have different experiences. Thus, we believe the interpretive perspective is the right choice.

For this bachelor's thesis, we used abductive reasoning. As we have had an iterative approach for developing empirical data and theory. We started our approach in theory and previous

research where we read and researched before heading over to the organization and gathered empirical data. This was done back and forth a couple of times and finally led to the results and empirical evidence stated later in this paper. (Le Duc,2007)

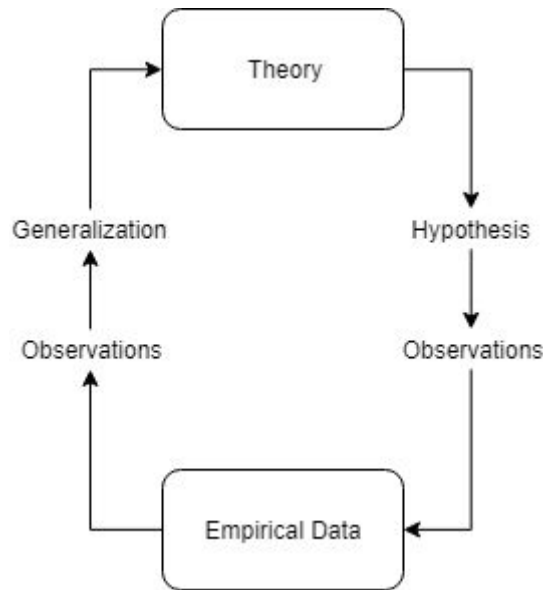


Figure 1: Model of abductive reasoning (own illustration)

2.2 Research Process

Our preunderstanding of IoT and IoT security in the three areas of updating, monitoring, and responding were limited to general knowledge as IoT is quite new to us. We have taken courses in IT security and organisational IT security but we did not know how this would apply to IoT security, although it gave us a firm foundation upon which to base our study on. With this in mind this is how we proceed to conduct our study.

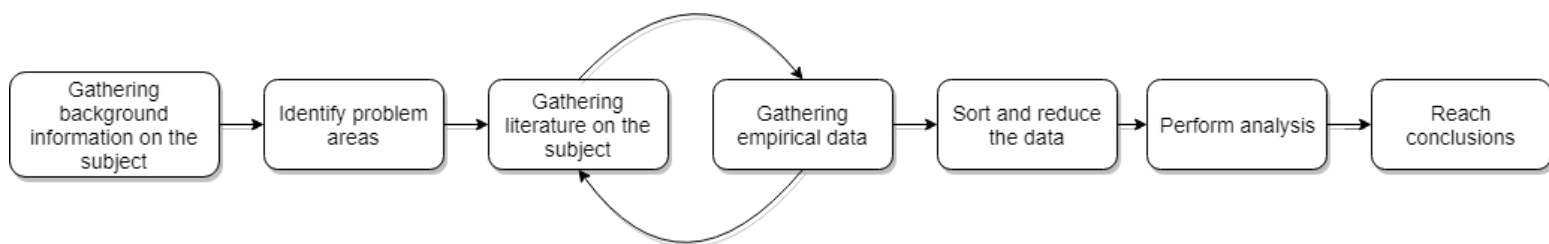


Figure 2: Model of the research process (own illustration)

2.3 Case Studies

For our bachelor's thesis, we chose to conduct a case study as we wanted to look at how the company participating in our study work with the areas we looked at and what challenges they face when working with these areas. For this bachelor's thesis we have chosen to call the

company Case Company, as we want to maintain the company's integrity and anonymity. Denscombe (2007) writes that case studies focus on a particular instance of a phenomenon and tries to provide an in-depth understanding of it. Case studies look at things in detail which a survey normally have trouble doing, and it provides a greater opportunity to delve deeper and into more detail to discover things which might not become apparent through more shallow and broader studies. Our bachelor's thesis fits into what Bryman (2011) describes as the typical case in which the goal is to capture the circumstances and conditions that the case experience regularly and describe them. The typical case he writes can be used to exemplify the case to a broader category as they constitute a context that could be commonly occurring. We believe that the company chosen for our bachelor's thesis fits this description as while it might not be many companies of this size in this field we believe it can be considered normal to those that are in this category of large companies working with IoT. Bryman (2011) mentions that it is questioned if case studies can be representative of anything other than the case itself which then questions if case studies can be generalized, which he answers is not possible and that researchers need to be aware of that fact. Denscombe (2007) also mentions this but also point out that case studies are still a single example of a broader class of things and that the findings of a case study can be generalized with similar findings in other case studies. We are aware of the problems that case studies have with representativity and generalization and our intention is to provide possible insight into the area chosen for this bachelor's thesis rather than providing fact.

2.4 Finding Literature

To search for previous literature we mainly used UniSearch, Linköping University's own database, and Google Scholar. Before we started searching we defined a few keywords, such as *IoT Security*, *IoT Security Management*, *Product Lifecycle Management*, and *Middle of Life Management*, which we used as a starting point. We then began searching using these keywords and when we found other terms used in the articles we found, for example *Cyber Resilience*, and the *CIA triad*, we added those to our searches.

2.5 Document Analysis

To start our bachelor's thesis, we chose to perform a document analysis on documents that were provided to us by the company participating in our bachelor's thesis. Denscombe (2007) writes that documents can be a source of data that is an alternative to questionnaires, interviews, and observation. The purpose of the document analysis was to serve as a base for our bachelor's thesis and the interviews we conducted. We did document analysis first to save time during the interviews so we did not need to spend time asking broader more basic questions about how the Case Company works with security in MoL management. This choice was also made to discover what areas we wanted to be explored further. It was also to

identify potential gaps in the information we need for our bachelor's thesis. With this information, we could ask more specific questions about their work rather than having to gather all data from interviews. We will perform a document analysis described by Bryman (2011) as *Official documents from private sources*. This type of documents, he explains, is used regularly by researchers that use observations or qualitative interviews to study organizations.

To make sure the documents we used were of the appropriate quality we used four criteria given by Bryman (2011). These are *Authenticity*, *Credibility*, *Representativity*, and *Meaningfulness*. **Authenticity** regards if we can trust the document's content and author. The **Credibility** criteria are used to check if the document is without errors or misrepresentations. A document's **Representativity** is estimated by checking if and how much the document fits in the category of documents it belongs to. **Meaningfulness** of a document is distinguished by how clear the content of the document is and if it is comprehensible. Bryman (2011) explains that even if the documents are authentic and meaningful for the researcher, they should not be satisfied with this and should still check the credibility and representativity of the documents.

The documents used in the document analysis were of two categories *white papers* and *website posts*. Most of these documents have been gathered from the Case Company's website, where they have a substantial amount of information, both the website posts, giving a brief glimpse of the area, and in the form of white papers in a more scientific manner, and the white papers, giving a more in-depth view into a specific area, where gathered on their website. Collectively these documents have given us a well-rounded view of the area. We have also conducted interviews by telephone with a couple of employees in the Case Company.

2.5.1 White papers

A white paper is a paper written by a company as a marketing piece based on facts (Graham, 2013). It is often at least 6-7 pages long but can be longer and is often written in a scientific manner without actually being scientific as it is more of a marketing piece (ibid.). In our case, the organization has written many white papers of which we used a few, which were relevant. These gave us a deeper insight into a specific area within the organization.

We assessed the white papers from the website according to the four criteria from Bryman (2011) and we have deemed that they fulfill all four criteria. We were aware that the White Papers are market pieces aimed to make to company look good, and this has been taken into consideration when analysing the documents to ensure a qualitative analysis. We have deemed them authentic as they come from a company working within this field for a long time that we have regarded as trustworthy. We have deemed these white papers credible as

they correspond with scientific literature we have found. We also believe they fulfill the criteria representativity for the same reason as the credibility criteria. We have found them to be understandable so we have deemed these to also be meaningful.

2.5.2 Website

The company participating in our study have also posted shorter texts on its website explaining the different areas they work in, general issues with those areas and how the solutions they as a company developed to deal with these. As they are a large company that works with different things, not everything was relevant for our bachelor's thesis but the post that did gave us more insight into what areas they work with security and what solutions they recommend.

We assessed the posts from the website according to the four criteria from Bryman (2011) and we believe that they fulfill the criteria of authenticity. As mentioned before they come from a company we have regarded as trustworthy and two of these posts have had contributors from researchers of Swedish universities, which increased their authenticity. We do think the posts are credible but as they are also made to market their solutions, because of this we had to keep in mind that they might have exaggerated the effectiveness of their solutions a bit or the severity of the issues they solve. But they were in line with other literature we have read so we do believe the posts can be deemed to be credible. We have deemed that these posts to fulfill the criteria of representativity as they are similar to other documents we have seen when we searched for the literature we needed for our bachelor's thesis. We have also considered these posts to fulfill the criteria of meaningfulness as we did not have much trouble to understand them.

2.6 Semi-structured Interviews

We had a clear focus area for data collection, security management within IoT, but as we were not sure what kind of answers we would get, we wanted flexibility so we chose to perform semi-structured interviews to be able to stray from the script if we found a new interesting area during the interviews while still giving some structure to the interview. Bryman (2011) writes that these are some of the strengths with semi-structured interviews, which makes it a good option to use. Denscombe (2007) writes that interviews are better suited for data collection when trying to explore a more complex phenomenon rather than gathering factual data. Interviews are more suitable when trying to get insights into people's experiences, opinions, feelings, and privileged information. Privileged information, he explains, is a depth of information that interviews are best at producing. Denscombe (2007) continues by stating that it is by interviewing people in special positions, that can provide insight as they have

knowledge others do not, that privileged information is gained. This is the reasons behind interviews being one of the chosen methods for this bachelor's thesis.

2.6.1 Performing interviews

The interviews performed for this bachelor's thesis were recorded, notes were taken as well as a safety measure in case there was any trouble with the recordings, which gladly we did not encounter, the recordings worked great.

We chose to use a one-to-one format for the interviews rather than group interviews for this bachelor's thesis. This is according to Denscombe (2007) the most common format for semi-structured interviews because it is easier to arrange, control and transcribe, although we made one change to the format. Denscombe (2007) describes the one-to-one format as being one interviewee and one researcher but we made the change that both of us were present although one of us was quiet and only took notes and the other one performed the actual interview, this was so that one of us could focus on taking notes while the other could focus on the questions.

The potential interviewees were chosen by the company participating in our bachelor's thesis according to who they thought would be able to give us a good insight into the areas we were studying. This was done after a meeting with the Case Company where we described and explained the purpose of our bachelor's thesis (For more information read section 2.3.3). We then contacted them and planned a date for the interview and then later actually performed interviews with those that responded and were available. We believe that contacting and asking the employees themselves was the better choice as it became more voluntary than if a superior would make them have an interview with us and we also believe this ensured that those who participated were more positive towards our study and that they were more interested in sharing their knowledge and experience

Two of the interviews were done by phone as the interviewees were situated in another country, which made face to face interviews inconvenient. This worked well, but not perfect, as the first interview was plagued by a bad sound quality which made it hard to hear what the interviewee said at times, which was remedied when we listened through the recording of the interview.

2.6.2 Transcribing Interviews

To help us transcribe the interviews we use a speech-to-text program. This was used to reduce the amount of time required for transcribing, as Bryman (2011) writes is a time-consuming task which we gladly avoided. This worked really well when the sound quality was of a high enough standard, which was not the situation on all of our interviews, the first interview

conducted was transcribed in a traditional manner, although the program worked well for our second interview. After the speech-to-text program had been used we also went through the interviews again to correct errors the speech-to-text program made. We then went through it one additional time to add comments on how the interviewees responded. Bryman (2011) explains that it is crucial to understand both what they said and how they said it to get a complete understanding of the interchanges in an interview. An example would be sarcasm as what is said means something vastly different when said sarcastically than regularly, another example would be to listen to if they like or dislike how something is done and thus getting their feelings towards the subject. This was something we tried to take into account as much as we could but was hard to actually accomplish for everything said, this due to the low audio quality of the interviews, and especially the first interview which had a lackluster audio quality which led to us not understanding all that was said. This led to us not being able to apply this method although we wanted to utilize it.

2.6.3 Snowball sampling

During this bachelor's thesis snowball sampling (Bryman, 2011) was utilized for finding persons to interview for the bachelor's thesis, as we did not have the opportunity to choose our interviewees ourselves as they were provided to us by the organization. Bryman (2011) also mentions that snowball sampling is a version of convenience sampling which is quite common in organizational research, which is another reason why we were comfortable using the snowball sampling method of sourcing interviewees. While sourcing people to interview for this bachelor's thesis we contacted one person working at the company we were interested in, we had the first meeting early on in the work with this bachelor's thesis to get a feel for each other, there we conversed about what we were aiming to research and what kind of persons we would need for interviewing and also what the organization actually does as we only had cursory knowledge into what they do. After the meeting, we sat down and compiled our preliminary research questions and some areas we wanted to investigate as a basis for the organization's choice of interviewees. With this basis, the organization was able to provide us with contact information to some people working at the organization he thought would be of value for our bachelor's thesis and we contacted them ourselves.

2.7 Email interview

After the phone interviews were completed we felt that we were missing some information that we needed, to solve this we contacted our first interviewee per email and asked a few questions to complement the answer we had already acquired through our phone interviews. This was very helpful as we discovered we really needed some more answers to questions that had arisen during our document analysis, as the documents did not always give satisfactory answers. With the additional answers gained from the email interview we felt satisfied and

contempt with the answers from the empirical findings we had and felt confident that we could do an interesting analysis.

2.8 Analysis Method

For this bachelor's thesis, we have used the three basic principles *sort*, *reduce* and *argue* (Rennstam, & Wästerfors, 2016) as well as *thematical analysis* (Bryman, 2011) which was used for the sorting. Before we started gathering data, we followed the advice given by Rennstams and Wästerfors (2016), which was to make sure not to gather too much irrelevant data. To ensure not to gather too much data at all, since it will require too much time to analyze, we chose three themes which we wanted to utilize, these themes were the ones used throughout this bachelor's thesis, *updating*, *monitoring* and *responding*. This made our jobs easier in the later stages of analysis. After the material was gathered it was sorted with thematical analysis, we sorted out the answers from the interviews and the findings from our document analysis according to *updating*, *monitoring* and *responding*, this made the data more easily manageable and easier to overview. Next, we reduced the data by the guidelines provided by Rennstam and Wästerfors (2016), which in practice meant that we did not use what did not fit in within our previously mentioned categories, this was also an iterative process and material was reduced in later stages when we discovered it was no longer relevant, this technique helped us reduce the data to just the relevant and essential data, the data that was left was all we needed for answering our research questions and fulfilling our purpose for the bachelor's thesis. Following that, we argued and analyzed the data following Rennstam and Wästerfors (2016) once again, this was mainly done by comparing our empirical data with our theory to see if we could verify or find discrepancies.

We followed the methods and guidelines by Rennstam and Wästerfors (2016) thus ensuring that the analysis would be done in a way that is easy and manageable for us and also that a good analysis was made. We chose to follow these guidelines since we believe they fit our bachelor's thesis. This by giving broad guidelines to work by so that we do not go in totally blind, while still giving us enough of a structure to base our analysis in. This analysis method is more loosely regulated, it gives suggestions on how to avoid the pitfalls in analyzing and gathering data rather than giving a strict rulebook to follow. We see this as positive because we wanted to leave the analysis open-ended to be able to analyze.

2.9 Reliability, Validity and Ethics

Reliability is a hard factor to ensure within qualitative research as research has high reliability if it can be made again and find the same answers (Bryman, 2011). This is hard to do in qualitative research as there are so many variables that change, as the specific researchers, respondents and a many other factors matters when reaching a conclusion in qualitative

research (ibid.). The conclusions will therefore, with a high probability, be quite different if some other researchers perform this research again.

While validity is an important factor in deciding whether an academic essay is viable it is also very hard to prove in qualitative research (Bryman, 2011). As this bachelor's thesis has a clear connection between the research questions and conclusions we believe this thesis has a high validity that at least is valid enough for a bachelor's thesis.

To make sure that the bachelor's thesis had been performed ethically in regards to the requirement of individual safety we followed the Swedish Research Council's (2002) research ethical principle. These are the information requirement, the requirement of approval, the requirement of confidentiality, and the requirement of usage. The interviewees were accordingly informed of this bachelor's thesis objective, their part in it and that they could withdraw from it if they change their mind. Aside from their job position and how long they have been working in that position, as that is the only information that is relevant for the bachelor's thesis, the interviewees were are anonymous. The interviewees confirmed the information they had given before publication.

The bachelor's thesis is also GDPR compliant and every interviewee has signed a consent agreement. In the consent agreement, the interviewee gives their consent to participate, that we will handle their information anonymously and correct, that they, at any time, can break the interview or end their participation in the research and, lastly, that we will handle all information according to the GDPR directive. GDPR stands for general data protection regulation and is a directive from the EU regarding "the protection of natural persons with regard to the processing of personal data and on the free movement of such data" (EU, 2016, p.1)

3 Theory

This is where we will present the theory and literature behind the Internet of things, organization, security, and Product lifecycle management more in dept. We will describe the three areas of security management of updating, monitoring, and responding, and we will present previous research done on security management.

3.1 Internet of Things

The Internet of Things is the collection of all connected devices, these can be anything from your toaster to your smartwatch. Tsiatis et al. (2019) define the IoT with this definition: "[t]he Internet of Things (IoT) is not a single new technology or phenomenon. It is a set of

technologies that combined deliver the promise of IoT. The origin of IoT is the Internet itself that connects computers and mobile devices” (p. 9). Where the promise is the vision of a global IoT based on solid technical vision and innovation (Tsiatis et al., 2019). As stated earlier this is what has led to why more research and more technical solutions is needed within the IoT, as it has all been mashed together in a jumble and just expected to work together. Although it has been an arguably good jumble as it has paved the way for many new and interesting technologies and solutions.

Zimmermann et al. (2015) writes that IoT revolutionizes businesses digital strategies by providing information. It integrates things, people, places and information. IoT also presents a way for businesses to measure, operate, analyze, and interact. To answer the question about how IoT architecture fits in the context of service-based enterprise-computing environments they write “The core idea for millions of cooperating devices is, how they can be flexibly connected to form useful advanced collaborations within the business processes of an enterprise.” (Zimmermann et al., 2015, p. 142). How these devices can collaborate with business processes is, however, never explained and the authors continue to propose a meta-model for an architectural solution to how businesses can perform IoT device management. Tsiatis et al. (2019) has observed this change as well, they mention how the IoT is transforming and changing much in the industry, thus leading to new and interesting technologies. The authors (ibid.) put this quite eloquently that the IoT is a “fundamental transformation that is redefining business processes and practices across a number of different industry and society sectors” (ibid., p. 3), this is a simile to the music industry’s change from analog formats to digital formats. The argument is that the IoT is as big a change for the industry as the digital music format was for the music industry. Some issues with the growing IoT is something that Yakimenko, Belov, Goncharuk and Stubarev (2018) raises, the IoT has never been developed as a whole instead it has been developed in parts by many different developers and manufacturers and now it is expected to all work together, which is a big issue as there is no agreed upon architecture for building these systems or devices. They (ibid.) further mention that “[a]nd even if independent systems are secure, we will have to cobble them together—and the resulting chain will only be as strong as the weakest link” (ibid., p. 572), as solutions to this the market has developed many solutions to solve the problem with bridging the different devices and systems, although these are often expensive.

3.2 Organization

Organizational culture is a vital part of how a modern organization is governed (Karlsson, Karlsson, & Åström, 2017). This means that it is a vital part of how security is managed in IT companies. Karlsson, Karlsson, and Åström (2017) define three measurements of information security in organizational culture: *rule following*, *trust*, and *participating*. **Rule following**

regards how well people in the organization follows security policies and rules. **Trust** regards how people in the organization perceive how well the organization works with information security and how they handle known threats. **Participating** regards what level of participation the people in the organization has in developing the information systems. Higher levels lead to better systems and more trust in the system. (ibid.)

3.3 Digital Security

Security is a vital and modern issue, as so much of what we do is through connected devices (Andress, 2014). Andress (2014) defines security as protecting our assets from attackers, viruses and even natural disasters. Andress (2014) gives the CIA triad as a model for discussing security.

3.3.1 CIA Triad

The CIA triad is a common type of definition of information security, it is an abbreviation of *confidentiality*, *integrity*, and *availability* (Lundgren, 2017). **Confidentiality** are sets of rules on how different information can be accessed. **Integrity** is to assure that the information is correct and trustworthy. **Availability** means that information can be accessed reliably by those authorized to do so. The information is secure if, and only if, each part of the information satisfies the requirements of confidentiality, integrity, and availability (Lundgren, 2017). Lundgren (2017) also mentions that more categories, such as traceability can be added for a more detailed view. We believe this could be used for analyzing the empirical results from a security perspective. With this, we have a basis for the analysis and concerns we will find.

3.3.2 Cyber Resilience

According to Aoyama, Naruoka, Koshijima, Machii, and Seki (2015), *Cyber Resilience* is the ability to cope with cyber-attacks and consists of four factors, gain knowledge from past events, effectively and flexibly respond to incidents, monitor threats and short-term developments, and anticipate potential long term threats and opportunities. They write that the number of studies on human contribution to cyber resilience is limited even though it is an important factor of cyber resilience, this is because earlier research has mainly focused on the reliability of equipment of infrastructure of organizations. Carias, Labaka, Sarriegi, and Hernantes (2018) states the approach to deal with the challenges of a connected world has evolved. The approach of cybersecurity, which has been focused on strategies for protection, has evolved into cyber resilience, which takes a more strategic long term approach to security. The lack of studies on organizational cyber resilience is also mentioned by Bagheri and Ridley (2017) who writes that the organizational aspects of cyber resilience has received less attention compared to research into technical aspects of cyber resilience. The authors write

that cyber resilience needs to focus on organisational and cultural aspects and that they are equally important to the technical aspects. Because of the lack of literature and that there is no accepted and practical method for cyber resilience it is harder for organizations to develop and implement it. This lack of literature is also something that we noticed as we had trouble finding literature for our bachelor's thesis. Most of the literature we found has been published quite recently and reflects what has been mentioned by Aoyama, Naruoka, Koshijima, Machii, and Seki (2015), and Bagheri, and Ridley (2017). This did make it hard to confirm the validity of our sources as there are so few studies on each area. We did however counter this with using peer-reviewed sources from authors that we deemed credible.

De Crespigny (2012) writes in an article that cyberspace is critical to organizations today. It is embedded into a lot of processes and is disconnecting from it is not a viable option. He writes that the financial risks that come from being connected are growing and are driven by 2 factors. The first is that cyberspace is always evolving and new opportunities present themselves. Organizations have a desire to adopt new technology quickly but this also brings unforeseen and unintended risks and consequences. The second factor is that cyber-criminals have become more organized and professional. De Crespigny (2012) writes that their financial rewards grow with cyberspace and that they are just as innovative as the organizations. All the benefits that organizations gain by utilizing cyberspace are also beneficial to hackers and attackers. Dealing with cyber threats is a problem for the whole organization and not only the parts that focus on cybersecurity. He writes that because the threats that appear can be unpredictable, unpreventable, and emerging fast, traditional risk management is no longer agile enough to manage the potential outcomes of cyber-attacks. No organization can be truly safe as the motivation behind attacks can also be ideological rather than the motivation being profit-driven. So organizations need to start building cyber resilience rather than relying on traditional cybersecurity. To do this organizations need to extend their focus from information CIA, and include other risks. These can include risks to reputation and unintended consequences from cyber activity. De Crespigny (2012) writes that cyber resilience cannot be sufficiently tackled alone, as the opportunities and risks with cyberspace are evolving so rapidly that risk management that tries to achieve security only through controlling and managing risks no longer provides the protection required. No organization can respond effectively on its own, and they must work with other organizations to leverage resources and knowledge of multiple stakeholders to enhance their cyber resilience. By partnering up, organizations can influence the adoption of best practices and by sharing knowledge the organizations can better understand the nature of the threats and its context to respond appropriately.

Linkov and Kott (2019) write that there are several approaches to improve organizations cyber resilience. They need to manage the complexity of their systems because catastrophic

failures in these systems appear from high complexity that can lead to unintended interactions the system designer did not count for. While there are cases where complexity can bring resilience to a system, in most cases, it will reduce it. They write that organizations need to choose the topology of their systems, how the parts of the systems and networks are placed and connected to each other, as this can increase a system's vulnerability. Linkov and Kott (2019) write that adding resources to a network can improve resilience. They give the example that increasing node capacity of power distribution and generation networks could reduce the probability of cascading failures and might speed up the restoration process. Another approach is to design for reversibility. All components of a system or network should be designed to be reverted to a safe mode when a failure occurs or a component becomes compromised. This means that the components should not cause further harm to their environment or itself. Linkov and Kott (2019) write that there need to be plans, preparation, and processes for human or artificial agents to be able to take measures to absorb, recover, and adapt and that these agents need to be always available. Humans and autonomous artificial agents are necessary and appropriate for different things. They write that human agents need to have the skills, processes, and resources available to them, and they must be rightly trained, motivated and prepared to act. Agents should also be interchangeable with multiple overlapping skill sets to improve the resilience of the organization. They continue that organizations need to consider their adversaries as they will most likely adjust their procedures and techniques to specifically defeat the organization's efforts to absorb and recover. Lastly, Linkov and Kott (2019) mention that organizations should perform an analysis of their resilience-enhancing methods to make sure their efforts do not have unanticipated resilience reducing effects. All measures need to be well analyzed to try and reveal any negative impact they can have on the organization's resilience.

3.4 Product Lifecycle Management

Product lifecycle management (PLM) is a tool for companies to gather useful data about their products during their lifecycle (Soós, Kozma, Janky, & Varga, 2018). This can have an impact on the success of their business processes. Soós, Kozma, Janky, and Varga (2018) explain that sharing information between the three stages of PLM can provide feedback during the whole lifecycle on the status of the device. As explained earlier, the different stages are the *Beginning of Life* (BoL), *Middle of Life* (MoL), and *End of life* (EoL).



Figure 3: Model of the product life cycle of devices (own illustration)

BoL contains planning, design, and development phases that take part before the device is deployed and it goes into the MoL stage. The MoL stage, which we will describe in more detail later, regards everything from a product has been deployed until it needs to be retired, where it will go into the EoL stage of deprovisioning and retiring.

Soós, Kozma, Janky, and Varga (2018) write that MoL for IoT devices consists of four kinds of actions, *reconfiguration*, *update*, *maintenance*, and *monitor*, that can change their behavior, capabilities, and check their status. During **reconfiguration**, the device's environmental setup or behavior gets changed but it will not get any new capabilities. When the device gets **updated**, it is often to improve the capabilities of the device. The authors write that most IoT devices need to be updated during their lifetime to be able to perform new tasks or perform previous tasks more efficiently. The devices also need to receive **maintenance** as it could otherwise lead to unnecessary expenditures from network failures or devices going haywire. Lastly, the authors explain that companies need to **monitor** any changes that happen in the device's behavior and environment. This allows for early intervention when problems are detected and to determine the status of their devices. Soós, Kozma, Janky, and Varga (2018) write that remote monitoring has become mandatory to support management actions of IoT devices.

3.5 Security Management

When we looked into the Middle of Life in product lifecycle management and cyber resilience, we found three areas which concern the management of security, which we will refer to as Security Management. These areas are the monitoring of IoT, updating IoT devices and networks, and responding to threats. Monitoring is specifically mentioned in PLM and cyber resilience, updating is mentioned as an area in PLM but we found that updating is loosely tied to responding within cyber resilience as a way of response rather than a specific area. Responding is a major part of cyber resilience and is not mentioned within PLM, which might be because of PLM does not focus entirely on security but all parts of the product life cycle, which include but is not limited to security.

3.5.1 Monitoring

Monitoring is the process of ensuring that only legitimate devices have access, that all software updates are authentic, and that only authorized people can access their data (Miettinen, van Oorschot, & Sadeghi, 2018). Miettinen, van Oorschot, and Sadeghi (2018) explain that there is a need for support for onboarding devices, continuing device management and deprovisioning of devices. Because IoT involves connecting a huge number of devices with a wide range of uses, they explain that the scale of IoT makes traditional solutions for management and association of devices obsolete. This is an issue that only gets

exacerbated by manufacturers using solutions for device management and onboarding, the process of connecting devices to a system. Keys for encryption need to be managed to keep data safe and interoperable key management solutions from different vendors are currently unknown. Miettinen, van Oorschot, and Sadeghi (2018) explain that this raises the burden on the owner of IoT trust domains, domains which can verify that users from that domain are legitimate because manufacturers of IoT devices often only provide basic and limited tools for managing of said devices. This leaves the domain owners, companies and individuals, to manually address keys, configuration and software management. The manufacturers sometimes remove user control from the owner of the device during software updates if they get any updates at all. The whole trust domain can be put at risk if the device becomes misconfigured.

3.5.2 Updating

Updating is the process of updating already delivered devices with new security measures or bug fixes. Teoh, Mahmood, and Dzazali (2018) explains that it is challenging for organizations to keep up with technology. The attacks on technology are ever-evolving and organizations need to update to the latest technology for defense. They write that attacks are both asymmetrical and multi-directional in cybersecurity. Attackers only have to succeed once while the organizations have to defend against every attack. Attackers can always benefit directly from new technology but organizations have to learn about it, plan a budget for it, and allocate resources. Van Oorschot (2018) mentions that device life expectancy is often between ten to twenty years, an issue with this is that this lifetime is often longer than the lifetime of the company developing the device, which leads to devices which are out in the field for years without getting updates. This has in turn led to subpar security with for example unauthorized over-the-air firmware updates (updates which can be done over the internet and does not require physical proximity to the device) as an solution to the security issue, but instead leading to more security issues (van Oorschot, 2018).

3.5.3 Responding

Responding is the process of responding to compromised devices. This area is closely related to monitoring, as this is area applies after the monitoring has discovered something amiss. When a compromised unit has been detected, a response is made. The response can be for example be taking the hacked device offline or restricting its communication access. Dorri, Kanhere, Jurdak, and Gauravaram (2017) have done a study on a smart home with a blockchain solution, a decentralized database storing the communications done in the smart home, which in this case is used for communication verification for its IoT devices by comparing the stored versions. In this case, the devices' communication was not allowed to

go through if it was not verified through the blockchain solution. These hacked devices can then, for example, be deprovisioned or reset and updated.

3.6 Previous Research

When we set out to find previously done research on our field, we could not find any exact matches. There was, however, previous research in areas close to what we are studying or parts of it. What we found is that the studies of nearby areas seem to be mostly technical studies, that focus more on the technical tools that can be used to monitor and manage IoT networks and devices. This correlates to what Bagheri and Ridley (2017) mentioned in their study that the organizational aspects of Cyber Resilience has been researched less than the technological aspects. We will now present a few of the studies which we thought were relevant for our bachelor's thesis as they touch on the areas we study.

3.6.1 Large Number of Different Devices

Ferreira, Soares, Jardim-Goncalves, and Agostinho (2017) writes about the difficulties of managing a large number of IoT devices and how different solutions are developed to deal with each target application. This creates a loss of productivity and increases costs. They write that consumers and businesses have a lot to lose from technical issues and this is perpetuated by the ever-increasing number of devices. The advantage businesses have from having interconnected devices providing information also comes with difficulties. This is because of the need for more efficient means to manage these devices. They write that this is a continuous issue that businesses have to deal with. Ferreira, Soares, Jardim-Goncalves, and Agostinho (2017) do propose a solution to this problem but it is an architectural and technical one. While we understand that this is a problem that requires a technical solution we believe it cannot be purely a technical one since these systems are described to only provide information. They are not the ones that maintain, update, and respond when issues occur within the system.

3.6.2 The Pillars of Security

We mentioned before that Teoh, Mahmood, and Dzazali (2018) in their study writes about how challenging it is for organizations to keep up with technology and that it takes time for the organizations to learn, plan and budget for it. While their study researches the implementation of cybersecurity they explain that security rests on three pillars within the organization. People, processes and technology. People need the right skills and share responsibility for security. Processes and technology need to be in place to support them. While they do not explain or give any examples of these processes it points towards that security cannot have a purely technical solution but also involves people and organization.

3.6.3 Technical Solutions vs Human Training

In a study about how to define a strategy for Cyber Resilience, Carías, Labaka, Sarriegi, and Hernantes (2019) explains how focusing investment in security can impact the success rate of cyber-attacks against IoT. They explain that companies are aware of the risks increasing as they embed technology into their processes but they are not prepared to deal with the possible implications of those risks, and cyber incidents can cause severe economic damage to a company through diminishing trust and reputation, loss of production and intellectual property, payment obligations, and fines. Companies need to their concept of cyber security for IoT into prevention, detection, response and recovery to prosper in the era of IoT. Carías, Labaka, Sarriegi, and Hernantes (2019) continues to explain that to build cybersecurity companies cannot only rely on technological tools because many problems in cybersecurity are caused by humans, and this they write cannot be underestimated. It can be hard for managers to properly budget cybersecurity for response and recovery plannings, awareness and education, and technological solutions. It is especially difficult if the managers to define a strategy if there is no previous experience with incidents that can indicate what effects and costs to expect. Carías, Labaka, Sarriegi, and Hernantes (2019) explains that current literature is looking to optimize investment measures in security for companies but that it mostly focuses on investments into technological solutions and how to balance minimum investment with enough protection. This means that the models brought forth forward does not consider the risk of humans that is present in a real situation. These studies they explain also approach security investment strategy with an economic perspective, and estimation of the cost of cyber resilience is often problematic.

Carías, Labaka, Sarriegi, and Hernantes (2019) researches how investment in technological solutions and employee training affect the success rate of cyber-attacks and management awareness. They come to the conclusion that both technical solutions and education are important but for different reasons and at different stages. Investment in technological solutions reduced the success rate of cyber-attacks faster but was not as effective long term. Employee education had more long term effect but was slower to see the results from. They also noticed that investment in technological solutions did not raise management awareness of security issues as much as employee education. Interestingly they noticed that when the focus was to invest more into technology, the budget could become smaller compared to a focus on employee education, because management became more aware when employees gained a higher level of knowledge, they could, therefore, allocate more resources to both education and technology. They explain that both areas are important to become cyber resilient and that a focus is one area means that the other area is still invested in but not as much as the focus area.

4 Empirical Findings

Here we present the case company, the interview respondents, the documents we received and our empirical findings from the interviews and document analysis. The empirical findings will be presented in the areas of updating, monitoring, responding, and the challenges with IoT Management that are overarching the three areas.

4.1 The Case Company

The organization we have researched for this bachelor's thesis is a global IT-company with its basis in Sweden, it has around 100 000 employees where around 12 000 is employed in Sweden, making it one of the bigger in the industry. This company was relevant to our study as it is among the leaders of information and communication technology which IoT networks are a big part of. This made this organization a clear option for us to contact and do our research on. The organization is one of the oldest in the area as well as having been in the industry since its beginning, thus being a trend and standard setter, making it even more interesting to actually get insight into the company.

4.1.1 Respondents

Interviewee A

The interviewee from the first telephone interview we performed has worked in the company for more than twenty years in the company and is currently holding the title as Expert Security Architecture Principal, and A has been in that position for five years. This interview lasted forty minutes. It was also with this interviewee that we performed the mail interview a week after we performed the first interview with per telephone.

Interviewee B

The second telephone interview we performed was with someone that has worked in the company for around twenty-five years and has had several positions over the years but is currently holding the position as Senior Specialist IoT Security which B has had for a few years. The interview lasted forty-one minutes.

4.1.2 White Papers

These are short summaries of the white papers (or WP for short) used in the document analysis for this bachelor's thesis. They are going to be described in short detail, we have also changed the names to the topics of the white papers instead of their title, as we want the organization to remain anonymous.

IoT Security - WP1

The IoT is rapidly growing along with its security concerns. Privacy and security are becoming more important within the IoT as it is being deployed and utilized in a widening array of cases of varying critical level, leading to increasingly hard security challenges. Proactive action is now a necessity to ensure the safety of the IoT. (Case Company, 2019b)

Cellular IoT - WP2

This paper describes the growth of the cellular IoT and how it is today along all spectrums of it, gsm to 5G, as well as giving explanations of different categories of IoT depending on criticality and size. (Case Company, 2019c)

5G security - WP3

Privacy and security are central for 5G to be utilized on a grand scale. 5G will now pioneer new security requirements for cellular networks due to becoming more and more popular among new businesses. (Case Company, 2019d)

Massive IoT - WP4

New standards on connectivity requirements lead to cellular networks with secure, diverse and reliable IoT services. (Case Company, 2019e)

Business, IT and networks - WP5

This paper describes how enterprise architecture can give excellent support for bridging the gap between IT, business and networks by giving six easy steps to follow and thus leading your business into the future. (Case Company, 2019f)

5G network security - WP6

This paper describes the security infrastructure of the 5G network, as well as the security architecture and standardization within the 5G system, lastly, it describes product security of 5G. (Case Company, 2019g)

Cognitive automation - WP7

With the growing rate of diversity within the IoT infrastructure and IoT application providers face a new height of complexity to uphold security and privacy to a high enough level. This paper argues that this should be done with cognitive automation. (Case Company, 2019h)

4.1.3 Website

As the website has information on a lot of different subjects, which we have decided to divide into the categories C1-8 (C, in this case, stands for category). The reason for the division is to make clear the different categories of security information that the Case Company has divided

its website into. Below are seven short summaries for each category of information on the website to give a brief look into the gathered information. In order to maintain the Case Company's anonymity the categories are not described in full, but instead, are summarized and worded differently than the original texts. Later in the text, these categories will be referred to by their assigned C1-8.

Cybersecurity Certification - C1

There were multiple posts about *cybersecurity certification* that we compiled into one document. These posts explain that IoT devices are separated into three categories when they are tested, which are named category one, two, and three, and that the Case Company have test labs in which it tests these three categories of IoT devices. These categories contain multiple different aspects like *authentication* and *privacy policies*, and the succeeding categories expands the previous category, this means that category two contains category one, and category three contains category one and two. (Case Company, 2019a)

Fault management and fault detection - C2

Here it is explained how the Case Company manages and detects faults within their networks. It introduces the necessary components in *fault management and detection*. It also presents three different ways to detect faults and what the Case Company believe is the future is for fault management and detection, *wait for users to report the faults*, *use test suites*, and *use of simple rules on monitored metrics that would trigger an alarm*. (Case Company, 2019a)

Identity management - C3

In a post on their website, the Case Company describes what *identity management* is and, what the challenges with it are, how it works with it and how the Case Company thinks it should be implemented. (Case Company, 2019a)

IoT security - C4

In this post, the Case Company describes the importance of security within IoT and presents four different factors that drive the need for IoT security, *Data-based decisions need reliable data*, *Different devices require different solutions*, *End-to-end ecosystems security*, and *Security management for IoT*. The Case Company also present four ways to start building trust in IoT, *trusted identities*, *trusted data*, *trusted connectivity*, and *privacy and confidentiality*. (Case Company, 2019a)

Secure IoT identities - C5

In a longer post on their website, the Case Company explains that there are a lot of different types of IoT devices with different needs and limitations, that IoT security is a major concern for businesses and that *Secure Identities* are a key part in that IoT security. The Case

Company present and explain a few key terms and concepts of IoT security, *device identity*, *crypto schemes*, *root of trust*, *TEE*, *device authentication and agreeing on keys*. The Case Company also explain a bit about how ecosystems and lifecycle management relate to IoT. (Case Company, 2019a)

Securing your Industrial IoT ecosystem against cyber threats - C6

In this post, the Case Company describes the challenges with *industry 4.0*, the fourth industrial revolution in which everything is connected, and that smart industries must rethink their security for it. The Case Company explains that there is a need for higher levels of security management on two levels, Horizontal, and vertical. The Case Company proposes that the best defense against cyber-attacks is a four-leveled approach, *Secure approach*, *Secure products*, *Security products*, and *Security operations and management*. Lastly, the Case Company explains why industry 4.0 will not be if the security challenges with IoT are not solved. (Case Company, 2019a)

Security Management - C7

On their website, the Case Company have two posts we compiled were the first one explains why *security management* is important and that the challenges with it will increase with the implementation of 5G cellular networks and IoT. The second post explains how their *security manager*, a system the Case Company developed, is and how it can help to manage IoT security. (Case Company, 2019a)

The importance of Network Security - C8

In this post, the Case Company discuss why it is important for operators to provide secure networks to gain trust. It also explains that threats and attacks against networks are evolving, some reasons why, and how their service can help to protect against these threats. (Case Company, 2019a)

4.2 Updating, Monitoring, and Responding

We will now start to present our empirical findings from our gatherings, we will weave together the three categories of empirical findings, and we will present them in the three categories, updating, monitoring, responding, and the challenges with IoT security management.

4.2.1 Updating

When asked about how they keep up to date with the latest threats against their IoT networks and devices they both mentioned that the Case Company does not to devices anymore, they are more on the network side nowadays, although the two see a need to stay up to date with

the newest threats, interviewee A emphasize that they need to have the latest and greatest security functionality in place. They both remark that the best way to stay up to date is not to just being able to actually update devices and networks already deployed, but rather, have a holistic security perspective of the whole process starting from development, and on all the domains from the device domain to the network domains. Interviewee A also mentions that a risk-based approach is utilized during development to be able to mitigate risks already in that stage, this is done in several different ways one way is that they have a team looking into open source software and see what vulnerabilities exist there, they have several other teams looking into different areas. In WP6 (Case Company, 2019g) these types of teams are called vulnerability assessment teams and are working hard to assess risks and prevent flaws from being released. All of this research that the organization does is the basis for keeping up to date against security threats.

When asked about the challenges with keeping up to date interviewee A talks mentions that it is not technical challenges, but more organizational. Interviewee A raises issues with devices being out in the field for years without updates A also gave us an example of A's water meter that has been going for eight years without an update. In WP1 (Case Company, 2019b) it also says that devices have a long lifetime, and that manual configuration is expensive which leads to a higher importance of being able to update over-the-air. This is also mentioned by interviewee B which said "In order to keep them in in in secure state you need to have the solution where you can update the device on air [and] over the air and then you of course need to make sure that correct software or firmware loading to those devices by having integrity and reaching checkpoints". It also raises the issue of the small storage space on IoT devices left out in the field, as it is hard to update a device if the storage is too small to store the update as well as the old firmware. This is iterated in WP4 (Case Company, 2019e) as well, as the updating process is often more demanding on the system and network than the other security measures, such as the controlling and monitoring of the device, system or network. A also mentions that one of the bigger challenges is that it is hard to actually predict what the next security threat will actually be, although that is something they are trying and hoping to do.

When asked about hardware updating B again said that devices are not something the Case Company really works with anymore, although, B mentions that it is important to keep the hardware up to date as well as the software. Since if the hardware is not secure how can the network be kept secure? B mentions that they have a device certification program that certifies devices and thus is deemed secure to use in the network. C1 (Case Company, 2019a) give further explanation of the cyber security certification program, the program is for certifying IoT devices so that IoT ecosystems and IoT network developers can work in peace without worrying if the IoT devices within the IoT network is safe and secure. Another way

the to ensure hardware and even network security is standardization which is something the Case Company advocates often, in WP1 (Case Company, 2019b) they argue that to be able to provide security, within the IoT, at a low cost standardisation is needed. Standardization is mentioned in nearly all of the White Papers in some form or another.

When asked about how it is to work with all the different kinds of devices that make up the IoT B explains the challenges of working with vastly different devices. B mentions that on very constrained devices the only way to see what is happening on them is to monitor how they behave, B continues to explain a bit about monitor (this will be more in depth explained in the next part). B mentions that an important aspect of constrained devices, as in this scenario, is over-the-air updating, B believes this to be important to keep up a satisfactory level of security and to maintain the integrity of the network and the devices.

4.2.2 Monitoring

When asked about how the organization monitors its IoT networks and devices from interference or hacking B answered that they have developed a security manager just for this purpose, which can monitor the traffic in the network and analyze it with a machine learning based analysis. A talks about software for monitoring that they are developing and we believe they are both talking about the security monitor. The continue to talk about the situation of the security monitor, how it can be used and utilized in monitoring IoT networks for suspicious behavior. On the website in empirical finding C7 (Case Company, 2019a) the security manager is explained in more detail, where it is explained as a way to monitor using security policies, and even has support for industry standard policies as ISO standards and GDPR.

When asked further about automated fault detection both interviewees answered that it was more on the network side. It may be used to detect strange behavior then raise an alarm so that an automated response or an operator may respond with the appropriate action. We could not get a clear answer in how much was automated and how much needed manual intervention. B laid emphasis on that it is not always feasible to disconnect a device as soon as it has been compromised, if it is a vital and important device there may be a lot of other mitigative actions that need to be taken before it can be disconnected and/or updated. As an example, B gave the hypothetical scenario of what if taking down the device would be life-threatening, if that is the case it may not be feasible to disconnect it without mitigating actions first. C2(Case Company, 2019a) gives further depth and explanation into fault management and fault detection. It describes five components within the area:

- A system for information collection, collecting up to date information about the system it is managing.
- A component for predicting and anticipating faults before they even would happen.

- A component for detecting components after they have faulted which have not been picked up by the system that is predicting and anticipating the faults.
- If the reason for the fault is not immediately clear there is a component for analyzing and identifying the reason of the fault.
- The last component is for recovery and prevention, which is in charge of recovering from the occurred faults and then making sure to prevent the fault from happening again.

Further C2(ibid.) gives details in how fault detection is done today and how the Case Company see the future of fault detection. Today they have three ways of detecting faults:

- Waiting for user to report the faults back to the company, which the Case Company say is the worst although simplest way of detecting faults, this is the norm in smaller organizations as the immediate cost is lower, although the cost over time may not.
- The usage of test suites, automated test done on the service checking the functionality as well as the availability. This can be utilized by doing frequent test often to quickly notice faults, although at a high cost, or doing the test less frequent and thus risking not detecting the fault in time.

For the future, the Case Company (2019a) see machine learning fault detection methods as the way to go. Where they see two different types of machine learning, supervised and unsupervised, the supervised method is trained by showing it known faults thus learning it to detect them, and the unsupervised method where it is trained by looking at the real system.

When asked about the impact of with IoT security management on the organization A said that it is probably of much help to have as it could help scale down the manual part of security operations and automate more. This can be seen as well in C2 and C7 (Case Company, 2019a) where security management, as well as fault detection, makes great use of automating more and thus optimizing costs.

When asked about the differences in traditional cyber security and IoT security both interviewees said that what makes IoT security harder is the number of devices, if you have a network of millions of devices it will be hard to find the single device that had been hacked. A mentioned that this might especially be a problem for devices that do not send data often as these will be even harder to discover. B explained that another issue is the lack of overall specifications and standards, which leads to networks consisting of very different types of devices, the diversity in the devices is not the only problem with diversity B iterates, diversity in the networks themselves is also a big issue as it makes general security solutions harder.

When asked about the differences in IoT security in cellular networks contrary non-cellular networks A said that from a device perspective it does not really matter as it is the same regardless of network type, A continued saying that what types of connectivity does not really

matter so long as you have connectivity. B mentions that the cellular network has a long legacy of security measures which makes it quite secure. In C8 (Case Company, 2019a) the importance of network security is described, the importance is described as vital in gaining the trust of the market and thus being able to earn more money and the advantage over competitors with less trust.

4.2.3 Responding

When asked about how the Case Company responds to attacks and compromised devices interviewee B answered that they had a response team that was notified as soon as something was discovered. They are then responsible for contacting everyone involved and affected by the incident. The other interviewee said that the responding is case dependent as it can concern both networks and devices, but when something is discovered it goes to the response team. There are some actions that can be done by automation but manual intervention is needed, and this goes accordingly to their policies on security management. A mention that more and more is done by automation, but that it will not be possible to fully automate it all since some of it will have to be done manually. In the whitepaper WP3(Case Company, 2019d), it is mentioned that the Case Company's Product Security Incident Response Team is responsible for actively and continuously monitoring newly found vulnerabilities and to make sure they are fixed as fast as possible. It explains that the most common security failure is to configuration shortcomings in the networks or poor operational procedures within those networks and that breaches often go unnoticed because of lacking monitoring. If an incident is discovered in those circumstances the investigation becomes very difficult, if not impossible to track down due to the lack of traceability. The flaws in the network can allow attackers to hide their tracks making it very difficult to detect and completely clean the network from damage. It is written in WP3(Case Company, 2019d) that prevention is not enough and that there need to be resources allocated to detect and respond to threats in a time sensitive manner after and during the attack and thus are activities with the goal of restoring the network to normal are vital. After a response is made it is important that vulnerabilities and weaknesses are removed to avoid being exploited once more.

When asked about what the largest challenge is with responding to attacks and compromised devices interviewee A answered that once a problem is discovered it is hard to know how many devices are actually compromised. As companies can have such a large number of devices of the same kind it can be difficult to check, recover and restore these, which can be time-consuming. A mentions that it can be hard to know what to do to with certain devices as it might not be possible to disconnect or turn them off to restore and update them as they might be critical in their use or the device might have critical data that needs to be saved before it is disconnected and restored. As an example, A mentioned a respirator. Turning it off a hacked one might be life-threatening but not doing so might be just as bad. This problem is

also mentioned by interviewee B who also mentions that is a reason why it is not possible to fully automate these kinds of processes as it can be hard to distinguish what response is the best for each case.

When the interviewees were asked if the responding could be done without a technician physically traveling to the location of the device B answered that it is very case specific and that is why you need to have a good understanding of the devices you are handling and that requires a good system to manage these devices. With good knowledge of your devices, you can detect faults and respond faster.

When we asked interviewee A about cyber resilience in the mail interview it was something A was familiar with but was not sure if cyber resilience was a concept that the Case Company works with and A had no experience working with it. A knew that cyber resilience is more about being reactive by focusing on detecting, responding and recovering and A believed some of their partner organization might be working with it but was not sure.

When asked about how they believe responding to compromised devices will be done in the future interviewee A once again starts to talk about how more will be done with automation and that more can be done remotely. Interviewee B believes that one important thing that will become better in the future is the response time. This is by moving response mechanisms closer to the devices through decentralization, a concept that is referred to as edge computing, this will let you discover and react faster to attacks.

4.3 Challenges with IoT Security Management

We will now also present more general findings that are not directly related to updating, monitoring, and responding but that are still having an impact on them or that are impacted by them. These are things about IoT that explains why our three areas are important in the first place or why they are needed.

One thing that we have noticed from both the interviews we have performed and the documents we have received is that the largest challenge with IoT is the enormous number of devices that need to be managed. Interviewee A mentions this when asked about what it is that makes monitoring IoT hard, and what the hardest part is to respond to compromised devices and attacks. It works when you have a few hundred or thousand different devices but when it gets to a few million devices it gets really hard to manage. Interviewee B also mentions this when asked about the difference between IoT security compared to normal IT security. Another difference was also the large variety of devices which in tandem with the huge number of devices made it really hard to monitor, update, and respond. This was also

brought up in the white papers and website posts. In C1(Case Company, 2019a) it is mentioned that it is of utmost importance to ensure that security is there as the number and diversity of IoT devices are growing. In C6(Case Company, 2019a) it is explained that the number of connected devices is multiplying rapidly on factory floors and that this increases the need for security strategies. Because there are so many more devices of such variety there is a wider area for hackers to attack that needs to be protected. The increasing number of possible attack angles because of the large number of devices is also mentioned in C8(Case Company, 2019a) and that network operators need to address the security gaps this brings to their networks. WP1 (Case Company, 2019b) explains that one of the problems with the number of devices is that it is hard to know who is who and this requires secure identification solutions. In WP4 (Case Company, 2019e) it is mentioned that one of the key challenges for IoT is to make sure networks are efficiently scalable to be able to handle millions of diverse devices.

WP4 (Case Company, 2019e) explains that in the future, every device that can benefit from having an internet connection will be connected and will help every industry and every person to reach their full potential. IoT can offer massive potential to improve safety, sustainability, and efficiency for industries and societies. This is also something that is a recurring theme in some of the other white papers. WP4 (Case Company, 2019e) focuses on how cellular networks is a massive part of IoT because it can cover a wide spectrum of different use cases for IoT. There are different types of cellular connectivity that can provide for the needs devices have, like slower, less energy consuming ones with high coverage or high-speed ones that cannot provide as much coverage. WP4 (Case Company, 2019e) explains that the IoT market is very diverse and covers everything from agriculture, smart cities, and industries, to consumers, transports, and environmental monitoring. It mentions that there are five key challenges for cellular IoT, the first one being that the cost of the devices is an enabler for many of the potential use cases. The second challenge is that devices need to run on batteries that have to last for a long time since replacing them in the field might not be possible or viable. The third challenge regards the coverage of cellular networks. Use cases like transportation and logistics need high coverage to work. The fourth is that networks need to be scalable to be able to deal with thousands or millions of devices. The last challenge is that networks need to be able to support the diverse spectrum of requirements the different use cases have.

A recurring theme in the white papers are security and privacy expectations from governments and the public, but information security has also become a top concern for organizations that are going digital. In WP6 (Case Company, 2019h) and WP1 (Case Company, 2019b) it is explained that it is important that the IoT is secure from the start as it starts off in a hostile environment, compared to when the internet began and everything relied

on mutual trust. WP1 (Case Company, 2019b) mentions that in a global customer survey, privacy and security were the main concerns after the media had raised the public's awareness. A few of the white papers mention that what can appear as harmless data, like room temperature or electricity consumption, can reveal personal habits, especially in combination with other data. WP3 (Case Company, 2019d) also mentions that the concerns about privacy are not only about data being stolen but also about the risk of mass surveillance, that we are being tracked through all the devices that will eventually exist everywhere. These concerns about privacy and security have led to regulation from governments and it is likely that IoT will continue to become more regulated. WP6 (Case Company, 2019h) mentions that there are problems with regulation and regulators walk a fine line between protecting the privacy and stimulating economic growth.

In the white papers, it is mentioned that cooperation between organizations is needed to be able to achieve IoT security. This is often mentioned through organizations working together to create standards. In WP3 (Case Company, 2019d) and C4(Case Company, 2019a) it is explained that to be able to ensure end-to-end security in IoT device manufacturers, network and platform providers, vendors, policy-makers, app developers and end-users must collaborate. Collaboration is explained to be fundamental to be able to become truly secure. When asked about this neither of the interviewees had any personal experience with these collaborations and B continued that it is correct that partners are needed. It is a huge ecosystem and that nobody can handle it alone.

When we asked interviewee A about if the Case Company focused more on technical solutions for security or if the focus was on employee training and education, A said that up until now there has been a clear focus on technical solutions but that is was beginning to change. If A measures that it used to be a 95 percent focus on technical solutions and 5 percent on training but that they now have an almost equal focus on both. The focus before was to bring forth requirements, design rules, and test tools but that they had recently put together a security organization that put together a learning portal and program to help build knowledge and awareness for developers. A also explained that A knew another large organization that had done this recently.

In WP1 (Case Company, 2019b) it is written that integrity and availability are more important than confidentiality in cyber-physical systems because losing control of locks, vehicles, or medical equipment would be far worse than having some eavesdrop on their data channels, although, A thought this was not the case and that confidentiality was still as important as availability and integrity. A similar thing is mentioned in WP3 (Case Company, 2019d) where it is mentioned that authentication methods like usernames and passwords need to be phased out due to not being secure enough. This is in regards to increasing threats against cellular

networks and that the damage from attacks could have an impact on public safety and not just be limited to business safety.

5 Analysis

In this chapter we will present our analysis of the results from our empirical findings in relation to the theory. We'll present our analysis for each area of updating, monitoring, responding, and how they are intertwined. Then we present challenges with IoT management that we found.

To iterate this bachelor's thesis aims to study how a large IT-company, the Case Company, can work with product safety management during the Middle of Life och IoT devices, thus we will compare our empirical findings with theory within the area and interpret and discuss using *sort, reduce* and *argue* (Rennstam, & Wästerfors, 2016) the sorting and reducing was made during the writing of the former empirical findings part of the essay and the arguing will now ensue in this analysis part using a thematic analysis method (Bryman, 2011).

5.1 Updating

Updating, an important but challenging area, if not prioritized and utilized attackers may soon get the upper hand. In our theory we mention Teoh, Mahmood, and Dzazali (2018) who explain that this is a challenging area and that the defense has to be ever-evolving to keep up with the, as well, ever-evolving attacks. This corresponds with our empirical findings, interviewee A lies heavy emphasis on the need to have the latest and greatest security functionality in place to outpace the attackers that have the same mindset. Teoh, Mahmood, and Dzazali (2018) also mention that attackers only have to succeed once against their target while targets as our Case Company has to protect themselves against every single attack aimed at them. They continue stating that attackers benefit from new and fresh technology while organizations need to take a while to learn the new technology, budget, and allocate resources from it. This correlates to our findings within our empirical findings as the Case Company works hard with learning new technologies, the have several teams working to learn and research new technologies. These teams called vulnerability assessment teams (Case Company, 2019g) are working with assessing vulnerabilities in different manners, interviewee A mentions that they have at least one team looking into open source software to see what vulnerabilities exist to see if they can mitigate this in their own software.

Another correlation between theory and practice is the issue with device life expectancy. Van Oorschot (2018) raises this as an issue as devices often have a lifetime of between ten and twenty years, making device lifetime often longer than company lifetime och the IT

companies and startups responsible for many of today's devices on the market. Interviewee A mention this as well, even giving us an example of A's private life, where A has a water meter in A's home which have been there for eight years without an update, WP1 (Case Company, 2019b) mention this as well and emphasizes the importance of over-the-air updating, although as seen in the theory part this has not always led to good solutions.

A lot of devices within the IoT have quite heavy restrictions on them, they need to have low energy consumption, since some IoT devices need to be online for a long time without recharging, thus setting restrictions on the performance of the IoT device (Andrea, Chrysostomou, & Hadjichristofi, 2015). The IoT devices then need to have low processing power and sometimes low storage, leading to restrictions on how complex algorithms they can perform and restrictions on the IoT devices, it is challenge actually finding lightweight enough and fast performing enough algorithms to keep up the security to a comfortable level (Sadeeq, Zeebaree, Qashi, Ahmed, & Jacksi, 2018). We see this as some critical challenges with security within the IoT, but the empirical findings lead to even more consequences coming from the limited performance of IoT devices. In WP1 (Case Company, 2019b) it is mentioned that the updating process suffers from this as well, when the devices storage is too small to actually fit the old firmware along with the update it is hard to do something so simple as actually updating the device, further in WP4 (Case Company, 2019e) it is mentioned that the updating process is often one of the most demanding processes a IoT devices is exposed to, leading to even more security issues. We see that the issue with limited performance on IoT devices is something that still persist within the IoT, as well as, something that both theory and practice has knowledge of and are looking into, the issue is that none seems to have come to a satisfied solution to this issue.

The Case Company has a device certification program for making sure devices are safe to use in your network or systems, this correlates with what Yakimenko, Belov, Goncharuk and Stubarev (2018) say, that there is no agreed upon architecture of IoT devices and IoT networks, which makes it hard to ensure security in the networks as one cannot know if the devices are secure. With the device certification program the Case Company aims to mitigate this problem by certifying devices, thus marking them safe to use in IoT networks, both for their own gain, but also for other network developers. This is a prime example of how reality works to mitigate problems discovered in theory, as the Case Company has realized this as an issue even before the paper used from the theory was released. Although Yakimenko, Belov, Goncharuk and Stubarev (2018) explain that when systems are cobbled together they are just as secure as the weakest link, we believe the device certification program from the Case Company, and other like it, will pave the way to an increased trust of devices that are secure, as someone with high reliability will be able to certify a device or service as secure smaller companies or organization can use these devices or services in good faith. Standardization is

another way that the Case Company ensure that working with the IoT is getting safer, or at least they are advocating strongly for it (Case Company, 2019b). In WP1 (Case Company, 2019b) they strongly advocate for standardization which correlates with what De Crespigny (2012) mention, that organizations can, by partnering up, influence the adoption of best practices within the industry.

5.2 Monitoring

Miettinen, van Oorschot, and Sadeghi (2018) defines monitoring as the process of ensuring legitimacy within the IoT network, this by making sure only trusted devices have access, that updates are authentic, and that only authorized persons are able to access data. Theory also states that there is a need for good monitoring and management of IoT devices and IoT network to maintain confidentiality, integrity and availability. This is a complex matter and leaves much responsibility on manufacturers of IoT devices and operators of IoT networks, such as the Case Company (ibid.). Case Company works with this in different manners firstly the Case Company has a relatively new piece of software called a security manager which is specifically made for monitoring IoT networks (Case Company, 2019a). The Security Manager works just as the theory defines monitoring, although it is a bit more specialized than just being able to monitor and authenticate the legitimacy of the IoT network and its IoT devices, as it has its basis in security policies such as ISO standards, and GDPR. Not only is the security manager monitoring the network, it also collects data and performs security analytics which in turn provides the Case Company (2019a) and the security manager with data and security insights which it can use to further mitigate future attacks and security holes. Secondly the Case Company (2019a) works with automated fault detection, which is a bit in the same category as the Security Manager although a little more general, as the Security Manager is an actual product. The automated fault detection works in many of the ways that theory states monitoring should be performed as it should. The automated fault detection even takes it a step further than just securing the authenticity and legitimacy of the IoT network (Miettinen, van Oorschot, & Sadeghi, 2018), as it also works with prediction of fault before it would happen (Case Company, 2019a). In this category or theme theory and reality is quite in line in what should be done and what actually is done, as the Security Manager and the automated fault detection both work in ways that Miettinen, van Oorschot, and Sadeghi (2018) actually says that monitoring should and needs to be done. The Case Company (2019a) believe that machine learning is the future of this area and we are inclined to agree with that as it would lead to less human interaction and more automation which interviewee A believes would lower the actual cost of the monitoring of the IoT networks and IoT devices. Miettinen, van Oorschot, and Sadeghi (2018) mention that manufacturers sometimes remove user control of IoT devices during updates and such, as this leads to a lowered possibility of misconfiguration, this can as well be applied on the operators of the network, if the network

work under a machine learning algorithm and is more or less automatized the human factor will be minimized and thus, we believe, will lead to more secure IoT networks which as well will be less prone to errors.

5.3 Responding

When we look at responding we see there is one theme that comes forth and that is the goal of making responses more and more automated as the number of IoT devices grow and to have less manual work. Both interviewee A and B mentioned that they utilize automated responding but not for everything as there are challenges with different IoT devices requiring different types of responses depending on how critical they are, for example an respirator might not be able to be taken offline without a backup immediately available. B tells us that they have a response team which is notified when something is discovered, this team is what performs the manual parts of the response. A does not believe that everything will be automated as complex cases need to be dealt with manually, but that automation is necessary because of the huge number of IoT devices. We find it interesting that there were little to no mentions of automation in regards to responding in literature. One of the few times we saw responding mentioned in regards to automation was in Linkov and Kott's (2019) study about cyber resilience where they write about the need for agents, human and artificial, to have plans, preparations, and processes to be able to deal with cyber-attacks against IoT devices and networks. They also mention that both human and artificial agents are necessary and useful for different things. These things are not specified in literature but interviewee A mentioned that automated agents are needed to deal with the more common responses to reduce the amount of manual work needed. Both interviewees found it hard to estimate how much work that was done automatically as they did not work with it directly and we could not find any evidence for that in the Case Company's white papers or their website. What is clear is that there are challenges for organizations in regards to responding to cyber-attacks and compromised IoT devices. According to both the identified literature and our case automation is the future in responding but it cannot replace all human intervention. Human agents are needed for complex situations where we cannot rely on automated systems to always make the correct decision.

5.4 The Three Areas Intertwined

During our analysis we used the three previously mentioned areas of updating, monitoring, and responding, but as the analysis went on we discovered that a lot of themes went across all three of the areas, leading us to draw the analysis that the three areas may not be as separated as we first thought, but instead, very much intertwined. When we asked about how to keep devices updated both interviewee A and B started explaining the importance of monitoring to find vulnerabilities so you could update and fix these vulnerabilities, as it was not possible to

just update all the devices when something in the network malfunctioned as this would not be feasible. When we further asked them questions about monitoring they both segued into talking about how to respond to attacks and compromised devices, as this was the natural step as this is what happens in reality when monitoring is utilized, it leads to a response of a malfunction of sorts. B also started talking about updating devices as response after vulnerabilities or weaknesses were detected, further leading to the intertwinedness of the areas. Then when asked about the level of automation in monitoring B continued to mention the problems with automated responding, as that was the perceived challenge with the area. These kinds of connections between the three areas were not that common in the white papers and the website posts, most likely because they had a different focus, as well as a quite narrow one, but we did see a similar connection in WP6 (Case Company, 2019g) where they merge monitoring into responding and updating. We did expect there to be some correlations between the areas of monitoring, updating, and responding as that coincides with the concept of cyber resilience as explained by Aoyama, Naruoka, Koshijima, Machii, and Seki (2015). But our understanding is that cyber resilience is not a widely used concept yet and we don't see these correlations as clearly in product lifecycle management and scientific articles on these subjects. When Soós, Kozma, Janky, and Varga (2018), Teoh, Mahmood, and Dzazali (2018), and Dorri, Kanhere, Jurdak, and Gauravaram (2017) mention these areas they described them like separate areas rather than them being intertwined. But when we actually looked at our empirical findings the areas were much more intertwined than theory lead us to believe. We nor believe that we have found enough correlations to show that there are connections between these areas, and that monitoring, updating, and responding are not things that organizations can choose to work with one or two of them but that they need all of them to be able to deal with the threats against IoT.

5.5 Challenges with IoT Security Management

We will now discuss more general challenges with IoT security management that is not directly connected to the areas updating, monitoring, and responding.

One recurring theme in empirical data we identified has been the large number of devices that IoT consists of, a number that will continue to increase according to all the data we have created and the literature we have read is the largest challenge within IoT. This is something that we have mentioned in all of the three areas of updating, monitoring, and responding. This is mentioned by both of the interviewees as the hardest challenge with IoT management. Miettinen, van Oorschot, and Sadeghi (2018) mention that the huge number of IoT devices makes traditional solutions for device management obsolete and Ferreira, Soares, Jardim-Goncalves, and Agostinho (2017) writes that businesses have a lot to lose from technical issues that are perpetuated by the increasing number of IoT devices. We believe that

this is the core challenge with IoT management and everyone seems to agree with that sentiment. There seems to be an understanding what needs to be done to deal with a large number of devices for example in WP3 (Case Company, 2019d) it was mentioned that systems and networks need to be designed to be more scalable to deal with all the devices and Ferreira, Soares, Jardim-Goncalves, and Agostinho (2017) proposes a technical and architectural solution to this problem. If the solutions proposed so far can solve this is not something we are able to answer but we think it is clear that both companies and researchers are aware of the problem and are trying to find a solution.

We believe one of the challenges organizations is to deal with the constantly evolving technology and the uncertainties that this brings. This is not only a problem that regards updating but also other aspects. In WP1 (Case Company, 2019b) it was mentioned that integrity and availability were more important than confidentiality for cyber-physical systems. The example given was that it would be a lot worse to lose control over vehicles than having someone eavesdropping on them. Cyber-physical systems were explained earlier by Van Oorschot (2018) and could include everything from powerplants to mobile phones. And if there was a scenario where we could choose to not risk losing control of a powerplant but instead risk privacy information, then we would choose to not risk control. But when we asked interviewee A about it, A did not agree that this is happening and that confidentiality, integrity, and availability were of equal importance. This is also what we have seen in previous research or literature, that all were equally important. As mentioned by Lundgren (2017), information is only secure if all requirements for confidentiality, integrity, and availability are fulfilled. But there probably is at least someone that believes that this will be the case at some point, as this has been published in the Case Company's white paper. This could be a real challenge for organizations working with IoT security management. Privacy concerns are rising as mentioned in WP1 (Case Company, 2019b) and that regulation is increasing in WP3 (Case Company, 2019d), so what happens if it becomes so that it is not viable to achieve the required security level? The possibilities we can see are that either development stagnates as organizations cannot fulfill the requirements for confidentiality, integrity, and availability, or what is stated by WP1 (Case Company, 2019b), that confidentiality becomes less important for cyber-physical systems. If this will actually happen is not something we can answer with the data we have collected in this bachelor's thesis but it is something that we believe can become a hard challenge for organizations if it were to happen.

Another theme we found was there has been a focus on technical solutions but not on the organizational aspects. When we tried to look up previous studies on the subject we were surprised by the amount of technical research compared to the organizational side. This we got confirmed by a study done by Aoyama, Naruoka, Koshijima, Machii, and Seki (2015) in

their study on cyber resilience and again in a recent study by Bagheri and Ridley (2017) where they confirmed what we had seen that there was a lack of organizational studies on cyber security and cyber resilience compared to the technical aspects. When we asked interviewee A about how their organization had prioritized developing technical solutions and employee training and education we got an answer that described a similar situation to what we have seen in the literature. This lack of research Bagheri and Ridley (2017) explains, makes it harder for organizations to develop and implement cyber resilience and this is also exaggerated by that there is no accepted method for implementing cyber resilience into organizations. But we did eventually find research on one of the organizational aspects. In a very recent study by Carías, Labaka, Sarriegi, and Hernantes (2019) looked at how investments into employee training and education affected the success rate of cyber-attacks compared to investments into technical solutions. In their study, they concluded that technical solutions saw more immediate results in reducing the success rate of cyber-attacks but that raising awareness and providing employee training resulted in more long term benefits. They believe that focusing investments into technical solutions were best made after a cyber-attack or a vulnerability is found and as then when the effects of that investment start to level out the focus should be switched to investment into employee training and education. According to Interviewee A, the organization used to have, what A estimated to be, a 95 percent focus on technical solutions and 5 percent left on employee training and education. But this A said has changed recently and they are now closer to both areas being about equal in importance. This seems to be in accordance with what Carías, Labaka, Sarriegi, and Hernantes (2019) described. We feel like this trend of focusing on technical aspects of security first correlates with what we have seen in literature and our case. The studies that we found that regards the organizational aspects of cybersecurity have been published recently and the focus shifts onto employee training have also been recent from our understanding. Employee A mentions that their organizational challenges with keeping up to date with the newest technology and the threats that it brings. Because of this, we think that there seems to a realization or understanding that there is a need for more research and development of the organizational aspects of cyber security and cyber resilience. Carías, Labaka, Sarriegi, and Hernantes (2019) mention that training and education employees also raise the awareness of security challenges in the management of organizations so we believe that we will see more and more focus on the organizational aspects as time goes on.

5.6 Analysis Summary

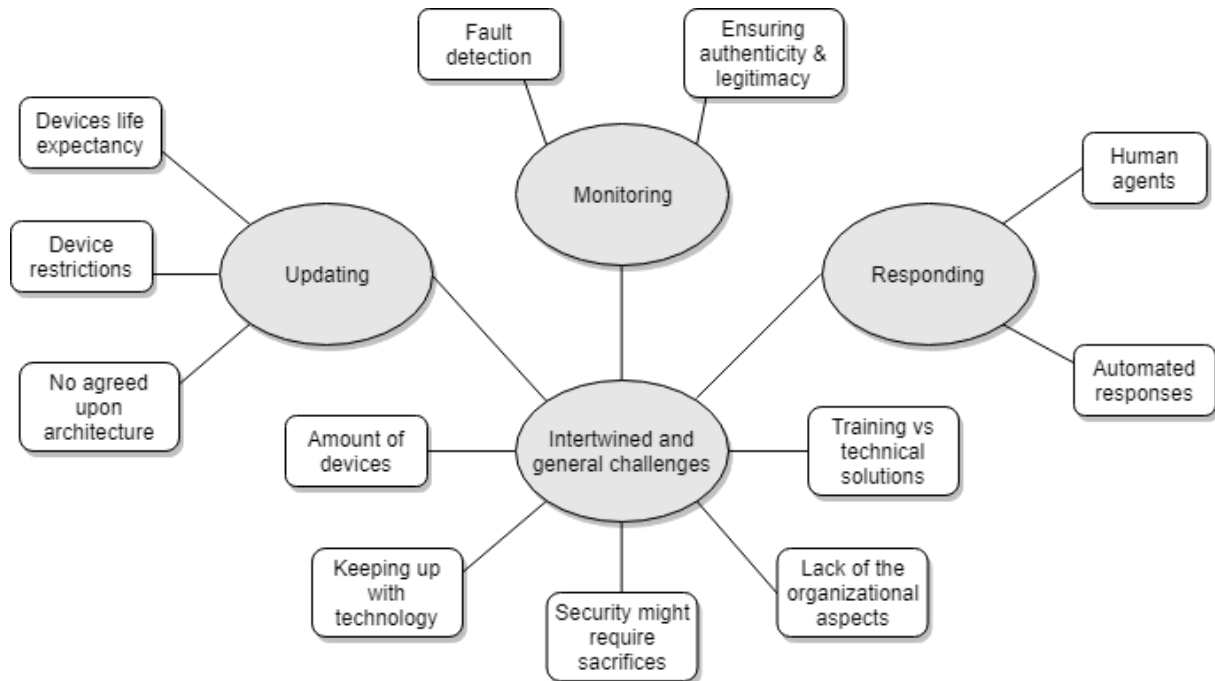


Figure 2: Model of the three areas and the themes found within them and general challenges (own illustration)

6 Conclusion

In this chapter we will present the conclusion we have reached by performing the analysis on our empirical findings and theory. We start this by restating the purpose of the bachelor's thesis and our research questions and then we present our conclusions for each of the three areas we have studied and the challenges with IoT management we found.

To give an answer to our research questions and purpose we will divide our conclusions into the three areas *updating*, *monitoring*, *responding*, and lastly the challenges of IoT management. Within these areas we will reason around the challenges with IoT security thus supplying an answer to our research questions.

6.1 Restating Purpose and Research Questions

Below we will restate our purpose, our research questions, and the goal with our bachelor's thesis, this is to give a clearer basis for our conclusion to stand on.

Our purpose:

With this bachelor's thesis we aimed to see how a large IT-company could work with security management within the IoT. This was mainly done with a focus on the three areas updating, monitoring, and responding. What we found was then compared to theory and previous research to draw correlations and analysis.

Our research questions:

- How can a large IT-company work with updating, monitoring and responding for IoT?
- What are the challenges of working with IoT Security Management?

Our goal:

The goal with our bachelor's thesis is to result in insight into how an organization can work with IoT MoL Security Management contrary to how it should be done according to theory and previous research. We will focus on priorities, policies, and guidelines over actual processes in how it is done in the organization compared to processes according to theory.

6.2 Updating

As we showed in the analysis theory and practice are on the same page regarding updating in many aspects, mainly that it is important to stay up to date with the latest and greatest security measures to ensure that attackers do not get the upper hand. The Case Company works with maintaining this in different ways, one way is their vulnerability assessment teams that works with keeping up to date with what vulnerabilities there are and thus the Case Company can mitigate these vulnerabilities before they become an issue. More challenges that practice and theory are agreeing on is the issues with the devices themselves, the limitations on the hardware on devices, with low power consumption and low storage, as well as the long life expectancy. Theory and our empirical evidence point to this challenge as a hard one for the IoT, and that it need to be worked on, the Case Company, in this case, does this in a couple of ways. Way one is that the Case Company has a device certification program for making sure a device is secure to use, we believe this is a good solution to the problem as it will ease the way for smaller companies and organization that do not have the resources in place that the Case Company has. The other way that the Case Company works with this challenge is that they are big advocates for standardization within the IoT, which we believe is a great idea for the IoT as it is dearly needed. We believe that the device certification program and standardization together will be what the IoT needs to become the secure and safe platform it dearly needs to be.

To summarize, firstly staying up to date is important and the Case Company has special teams allocated for this, secondly device limitations and life expectancy is challenging and the Case

Company has a device certification program for certifying secure devices and are big advocates for standardizing the IoT.

6.3 Monitoring

In the analysis we raised two challenges with monitoring that is exclusive to monitoring, the first one is the challenge with ensuring the authenticity and legitimacy of the network, its devices and the communication within. The Case Company has developed a Security Manager to mitigate this challenge in a good way, the Security Manager will ensure the authenticity and legitimacy of the network and its communications. This is quite a new technology only just starting to be sold to a couple of other companies, but we believe that this is a start in the way to monitor IoT networks in a suitable and secure manner. The second challenge we discovered is fault detection, this is a complex matter, especially in the giant IoT network that exists out there. The Case Company has started developing automated fault detection to automatically detect these faults without humans being needed to actually notice the issues, with less human interaction needed the monitoring will become cheaper and more available for more companies. They are as well working with automating as much as possible for the former mentioned cost reasons as well as trying to automate the responding as well.

To summarize we found two challenges within monitoring, ensuring authenticity and legitimacy in giant IoT networks, and fault detection, the Case Company works with these challenges with a Security Manager for the former and with automated fault detection for the latter.

6.4 Responding

In the analysis we found one main challenges within responding, which was the need to automate more, this is for keeping the cost down. With more automated response less human intervention would be needed and thus it would be cheaper as it is much more expensive to have an employee make a manual response than having an automated response through and automated system. This is what the Case Company is working with, automating as much as possible. They have a response team which is in charge of responding to faults and attacks, but all our empirical findings show that Case Company is aiming for automating as much as possible. A smaller challenge, although and increasingly important one, arose here, sometimes a device is not feasible to automatically take down if at fault, that is why everything cannot be automated.

To summarize we found one main challenge within responding, the need to automate more to keep costs down, the Case Company is working with automating as much as possible they as well have a response team working with the manual parts of the response. A secondary

challenge is within critical devices, as a critical device might not be able to be taken offline, which what the response team is responsible for.

6.5 Challenges with IoT Security Management

As we mentioned during the analysis there are multiple challenges with IoT security management that are not directly tied to the areas of updating, monitoring, and responding. These were mentioned both by literature and by the empirical data we created.

The first challenge we mentioned was that one overarching issue with IoT management was that there is an incredibly large number of IoT devices that need to be managed, which is hard with the amount of devices today and will be even harder in the future with even more devices. This was stated by one of the respondents in the interviews. “The scale is totally different compared to many other other security systems because of the amount of the devices.”(Interviewee B, personal communication, 8 april 2019). This created different problems for different areas and was solved in different ways by the Case Company. These problems were also given different technical solutions in research while research on organizational solutions was limited. But everyone seems to agree that this is the core issue with IoT.

Another challenge we found was that the ever-evolving technology brings uncertainty. Threats need to be predicted and reduced in advanced even if there might never actually become a realized threat. Due to a statement of weighting the different needs for security differently in some of the empirical data but not in literature, we concluded that organizations and researchers need to be aware that it might come to a point where it is not viable to uphold the highest level of security without some sacrifices and they need to be prepared to face that challenge if it were to become reality.

Lastly, we found a correlation between our empirical data and previous research, the focus on the technical aspects of IoT security has begun to change towards a more equal focus between the technical and organizational aspects. We looked at employee training versus technical solutions and according to the email interview that we performed, the change towards an emphasis on employee training and education in the industry has only begun recently. “Until now I see that we have more focused on tech solutions like requirements, design rules and test tools, but recently we have from a security organization put together a learning portal/program to help developers to build knowledge and awareness.”(Interviewee A, personal communication, 20 april 2019)According to Carías, Labaka, Sarriegi, and Hernantes (2019), this change has also been seen in the literature. The authors also state that employee training and education will raise awareness of the importance of security in the organization

than applying technical solutions and provide more long term benefits, but this is something we were not able to confirm. We believe that it is probably due to it being too early to confirm if the effects they mention as the change has been too recent to truly see the effects.

6.6 Our Contribution

The goal with this bachelor's thesis was to research how an IT-company can work with security management within the areas updating, monitoring and responding and the challenges with this. During the course of this bachelor's thesis we managed to discover how an IT-company can work with these areas as well what the challenges are. With this we hope to raise awareness that this clearly needs more research to satisfy the knowledge gap we have found. We also hope this bachelor's thesis can be used as a stepping stone to walk further into the pond that is IoT security management within the information systems field.

7 Reflection

In this section we will reflect on the strength and weaknesses of our bachelor's thesis, what we believe was done well and what could have been done better. We will discuss the generalizability of our bachelor's thesis and present areas for future research.

7.1 Reflection

The case study we performed was on a large IT-company based in Sweden and has covered two interviews, one mail interview, Seven white papers, and eight categories of website posts. We started our bachelor's thesis wanting to answer how organizations work to keep IoT secure and discovered that this is something that both researchers and the industry is trying to solve. We found out that the challenges that comes from implementing IoT is agreed upon, by researchers and industry, but what is actually needed to solve them differ between them.

A weakness in our bachelor's thesis is that we could only get hold of two interviewees which limits the number of insights we could have received. This made us rely more heavily on the document analysis then we would have preferred, but we did receive a good number of documents and these served us really well as a source of empirical data even if we had to rely more heavily on the document analysis we performed due to having few interviews. If we could have performed at least two or three more interviews, as well as potentially interview people in other positions, we could have gotten a better understanding of the collaborations between companies and how they work with employee training or how they set policies for IoT security. Another weakness we see is that we found cyber resilience late in our bachelor's thesis, if we would have found it earlier we think that it would possibly become a larger part

of our bachelor's thesis. We do believe that there are strengths to our bachelor's thesis, such as that the literature we have used has been published in recent years, most coming from 2017-2019, and that the case we have studied is very relevant to study as they are one of the leading companies in this field. The field we have studied has become very relevant in recent years even if the concept of IoT is not something new, as the field we have been studying is quite new we believe that our bachelor's thesis is very relevant for what is happening within IoT security today.

We believe that the result of our bachelor's thesis can be interesting for IT-companies of similar size that are looking at implementing IoT devices into their organization. Because we looked at the challenges on a high level, and because of that the literature we found and the empirical data that was created correlated and agreed on the challenges but not the solutions for IoT management, we believe that the result can be generalized somewhat to other large IT-companies. Because our bachelor's thesis is limited by the scope and the case we have studied we believe it cannot be used as a fact of what challenges an organization might face when implementing IoT, but even if other organizations can come to implement different solutions we believe that according to the result of our bachelor's thesis that there are challenges that they are likely to have and have to prepare for. We believe that researchers and students within information systems may as well find our bachelor's thesis of interest. This bachelor's thesis is, as stated above, in a new and fresh area with not much prior research which leads us to believe that it may be of interest as a starting point in future research for students and researchers within the information systems area.

7.2 Future Research

We believe that we, in our bachelor's thesis, only touched the surface of the field of IoT security and IoT security management. As stated by Bagheri and Ridley (2017) there is limited research done on the organizational aspects of cybersecurity and cyber resilience which we also discovered during this bachelor's thesis. We believe that there are a lot of different areas where future research is needed for the organizational aspects of IoT security and IoT security management. There are multiple mentions of that IoT security is different from normal IT-security which is poorly described why and we have only been able to touch on some aspects of those differences in our bachelor's thesis, for example the huge difference in the number of devices. What we have seen is that most of the research we have seen, within organizational research, have been on a general level and we believe that more in depth research across both the areas of updating, monitoring, and responding which we have looked at for our bachelor's thesis but also other aspects of IoT security that and IoT security management.

8 Reference List

8.1 General references

Albrecht, K., & McIntyre, L. (2015). Privacy nightmare: When baby monitors go bad [opinion]. *IEEE Technology and Society Magazine*, 34(3), 14-19.

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, July). Internet of Things: Security vulnerabilities and challenges. In *Computers and Communication (ISCC), 2015 IEEE Symposium on* (pp. 180-187). IEEE.

Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress.

Aoyama, T., Naruoka, H., Koshijima, I., Machii, W., & Seki, K. (2015, May). Studying resilient cyber incident management from large-scale cyber security training. In *2015 10th Asian Control Conference (ASCC)* (pp. 1-4). IEEE.

Bagheri, S., & Ridley, G. (2017). Organisational cyber resilience: research opportunities. In *ACIS2017: Australasian Conference on Information Systems* (pp. 1-10).

BBC(2018, 16 september). Cyber attack led to Bristol Airport blank screens. BBC. Accessed on 2019-03-25 from <https://www.bbc.com/news/uk-england-bristol-45539841>.

Bryman, A. (2011). *Samhällsvetenskapliga metoder*. (2., [rev.] uppl.) Malmö: Liber.

Carías, J., Labaka, L., Sarriegi, J., & Hernantes, J. (2019). Defining a Cyber Resilience Investment Strategy in an Industrial Internet of Things Context. *Sensors*, 19(1), 138.

Carias, J. F., Labaka, L., Sarriegi, J. M., & Hernantes, J. (2018, June). An Approach to the Modeling of Cyber Resilience Management. In *2018 Global Internet of Things Summit (GloTS)*(pp. 1-6). IEEE.

Darabian, H., Dehghantanha, A., Hashemi, S., Hodayoun, S., Choo, K-KR. (2019). An opcode-based technique for polymorphic Internet of Things malware detection. *Concurrency Computat Pract Exper*. <https://doi.org/10.1002/cpe.5173>

Denscombe, M. (2007). *The Good Research Guide: For Small-Scale Social Research Projects* (third edition), Milton Keynes: Open University Press.

de Crespigny, M. (2012). Building cyber-resilience to tackle threats. *Network Security*, 2012(4), 5-8.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In *Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017 IEEE International Conference on (pp. 618-623). IEEE.

EU (4 May 2016) Official Journal of the European Union, Vol. L119 , pp. 1-88

Ferreira, J., Soares, J. N., Jardim-Goncalves, R., & Agostinho, C. (2017, May). Management of iot devices in a physical network. In *2017 21st International Conference on Control Systems and Computer Science (CSCS)* (pp. 485-492). IEEE.

Greenberg, A (2017) 'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID. *Wired*. accessed on 2019-03-04 from <https://www.wired.com/story/crash-override-malware/>

Graham, G. (2013). *White papers for dummies*. John Wiley & Sons.

ITU (2005) "The Internet of Things". *ITU Report*

Karlsson, M., Karlsson, F. & Åström, J. (2017). Organisationskulturens påverkan på informationssäkerhetsarbetet. In Hallberg, J., Johansson, P., Karlsson, F., Lundberg, F., Lundgren, B. & Törner, M. (Red.), *Informationssäkerhet och organisationskultur* (p.25-40). Lund: Studentlitteratur.

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, 50(7), 80-84.

Le Duc, M. (2007). Induktion, deduktion och abduktion. Metodhandbok som tankekarta. [Online]. Available at: <http://www.leduc.se/metod/index.html>. Accessed on 2019-05-14.

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In *Cyber resilience of systems and networks* (pp. 1-25). Springer, Cham.

Lundgren, B. (2017). Vad är säker information? In Hallberg, J., Johansson, P., Karlsson, F., Lundberg, F., Lundgren, B. & Törner, M. (Red.), *Informationssäkerhet och organisationskultur* (p.199-214). Lund: Studentlitteratur.

Miettinen, M., van Oorschot, P. C., & Sadeghi, A. R. (2018). Baseline functionality for security and control of commodity IoT devices and domain-controlled device lifecycle management. *arXiv preprint arXiv:1808.03071*.

Myers, M. (1997). Qualitative Research in Information Systems. *MIS Quarterly*, Vol. 21, No. 2, pp. 241-242. MISQ Discovery, archival version, June 1997.

Rennstam, J. & Wästerfors, D. (2016). Att analysera kvalitativt material. In Ahrne, G. & Svensson, P. (Red.), *Handbok i kvalitativa metoder* (p.220 - 236). Stockholm: Liber.

Sadeeq, M. A., Zeebaree, S. R., Qashi, R., Ahmed, S. H., & Jacksi, K. (2018, October). Internet of Things Security: A Survey. In 2018 International Conference on Advanced Science and Engineering (ICOASE) (pp. 162-166). IEEE.

Sagirlar, G., Carminati, B., & Ferrari, E. (2018, October). AutoBotCatcher: Blockchain-based P2P Botnet Detection for the Internet of Things. In 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC) (pp. 1-8). IEEE.

Soós, G., Kozma, D., Janky, F. N., & Varga, P. (2018, August). IoT Device Lifecycle—A Generic Model and a Use Case for Cellular Mobile Networks. In 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 176-183). IEEE.

Statista (2019), Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions), accessed on 2019-03-04 from <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>

Symantec. (2018). Internet security threat report. Vol 23.

Symantec. (2019). Internet security threat report. Vol 24.

Swedish Research Council, V. (2002). Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning.

Teoh, C. S., Mahmood, A. K., & Dzazali, S. (2018, August). Cyber Security Challenges in Organisations: A Case Study in Malaysia. In 2018 4th International Conference on Computer and Information Sciences (ICCOINS) (pp. 1-6). IEEE.

Tsiatsis, V., Karnouskos, S., Holler, J., Boyle, D. and Mulligan, C. (2019). Internet of Things. 2nd ed. Elsevier.

Van Oorschot, P. C. (n.d.). Internet of Things Security: Is Anything New? *IEEE SECURITY & PRIVACY*, 16(5), 3–5.

Yakimenko, A. A., Belov, A. I., Goncharuk, P. S., & Stubarev, I. M. (2018, October). Development Platform for Controlling the Infrastructure of the Internet of Things. In 2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE) (pp. 572-578). IEEE.

Zimmermann, A., Schmidt, R., Sandkuhl, K., Jugel, D., Möhring, M., & Wißotzki, M. (2015). *Enterprise architecture management for the internet of things*. Gesellschaft für Informatik eV.

8.2 Case references

Case Company (2019a). Company website, accessed on 2019-04-24.

Case Company (2019b). *White Paper 1*. Company website, accessed on 2019-04-24.

Case Company (2019c). *White Paper 2*. Company website, accessed on 2019-04-24.

Case Company (2019d). *White Paper 3*. Company website, accessed on 2019-04-24.

Case Company (2019e). *White Paper 4*. Company website, accessed on 2019-04-24.

Case Company (2019f). *White Paper 5*. Company website, accessed on 2019-04-24.

Case Company (2019g). *White Paper 6*. Company website, accessed on 2019-04-24.

Case Company (2019h). *White Paper 7*. Company website, accessed on 2019-04-24.