



16-01-2017

Internet of Things: Security guidelines for management

Master Thesis

Cand.Merc.IT - MSc in Business Administration and Information Systems

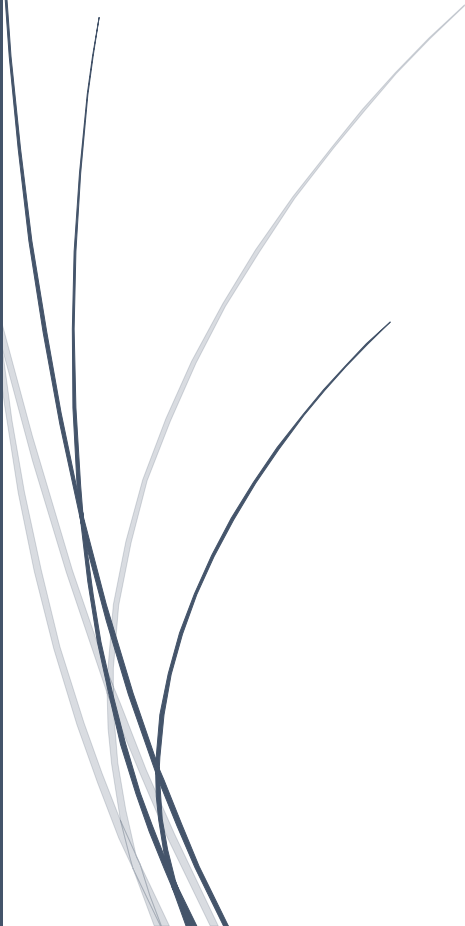
Copenhagen Business School

Mikael Hansen

Supervisor: Jacob Nørbjerg

Keystrokes: 181,017

Pages: 89



Abstract

This report sets out to create a set of guidelines for organizations to use when they are thinking about implementing Internet of Things solutions in their organizations and do not know how to handle the IoT technology. The guidelines are created by reading the scientific literature on the IoT topic and then going in depth with the areas of which IoT can pose a threat to the company's security or otherwise be a nuisance to the company.

By reading, the literature with a hermeneutic approach it is secured that there are no topics left untouched and with every aspect of IoT explored it was possible to create a framework, which includes all the essential topics found in the literature. This framework is the basis for how the theories were conceptualized in the context of IoT. By conceptualizing the theories a set of statements were made based on the literature, these statements were tested with expert knowledge in the security field.

The tests conclude that most of the hypotheses were verified, and therefore useful as a whole or broken down in to individual points in the guidelines. The findings were that the guidelines need to include regular IT security measures such as encryption, access control, privacy and regular network security theories such as network segmentation.

Furthermore, the results found showed that security measures are not everything the organization needs to be aware of. They also need to attend to organizational structure and readiness as these topics among others came fourth: strategy purpose, risk assessment, partners and manufacturers. Evaluating these can help secure a smooth implementation of IoT in the organization alongside having a secure IoT system.

Answering the research question: How can companies handle the introduction of IoT devices?

They can use the set of guidelines outlined in this report, to raise awareness and be skeptic about introducing new technologies without thinking about the potential consequences it can impose on the organization.

Table of content

Abstract.....	1
Chapter 1 Introduction	4
1.1 Introduction	4
1.2 Statement of intent.....	7
1.3 Problem Definition.....	8
1.4 Delimitation	8
Chapter 2 – Related research and theory.....	8
2.1 Related research	8
2.2 Theory	9
2.2.1 IT Security.....	9
2.2.2 IoT Flower model	12
2.2.3 Standards	15
2.2.4 Risk.....	17
2.2.5 Organization processes and Leadership	18
2.3 Conceptual Framework.....	21
2.3.1 Security	21
2.3.2 Internet of things	21
2.3.3 Standards	22
2.3.4 Risks	22
2.3.5 Organizational structure and leadership	22
2.3.6 Conclusive remarks	22
2.4 Guidelines and challenges for security	23
Chapter 3 – Methodology	24
3.1 Approach.....	24
3.2 Empiricism.....	25
3.3 Validity and reliability	26
3.4 Scientific positioning	27
Chapter 4 Literature review	29
4.1 Architecture & IoT security:	32
4.2 Data handling:	32
4.3 Network:	33
4.4 Privacy:.....	33

4.5 Cryptography	34
4.6 Access control:	35
4.7 Literature review conclusion:	36
Chapter 5 Analysis and test of results.....	36
5.1 Analytic structure.....	37
5.2 Literature findings.....	38
5.3 Analytical model.....	44
5.3.1 Security	45
5.3.2 Internet of Things.....	47
5.3.3 Risks	48
5.3.4 Standards	49
5.3.5 Organizational structure and leadership	51
5.4 Test of results.....	53
Conclusive remarks	58
Chapter 6 Results	59
6.1 Guidelines	59
1. Strategy	59
2. Organization.....	61
3. Network and security.....	62
6.2 Discussion.....	64
Chapter 7 Conclusive remarks	64
7.1 Conclusion.....	64
7.2 Reflection	68
7.3 Perspectivation	69
References	70
Figures and tables	74
Appendices.....	74
Appendix 1 - ISO 27000 Series	74
Appendix 2 – Literature matrix (reading guide).....	77
Appendix 3 – Interview guide	78
Appendix 4 - ISO versus IoT Map	79
Appendix 5 – Interview 1	80
Appendix 6 – Interview 2	86

Chapter 1 Introduction

1.1 Introduction

Internet of Things (IoT) is not a new phenomenon in regard to IT, but the phenomenon of billions of devices being interconnected some way or another is only just about to flourish.

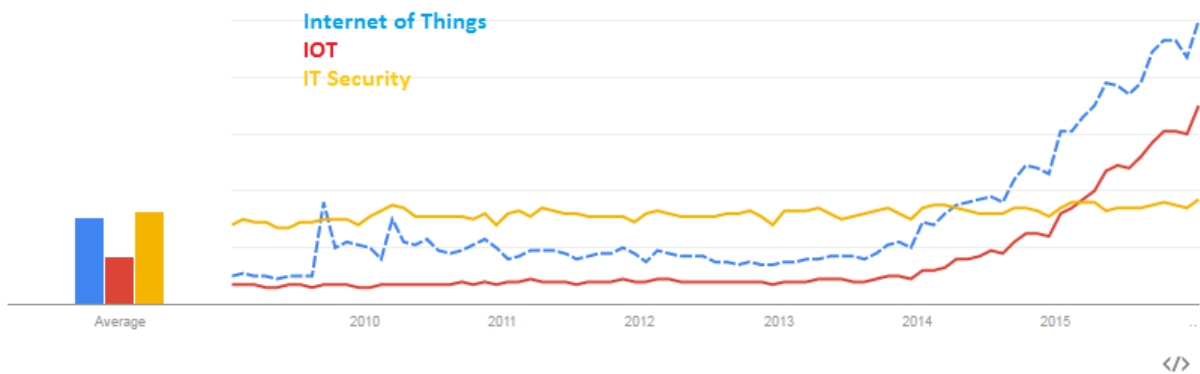
Kevin Ashton first mentioned the phenomenon “Internet of Things” in 1999 during his work at Procter & Gamble. Ashton was a researcher at MIT, at the Auto-ID department, which was the first ones to have a conference on IoT (Ashton, 2009). In line with Moore’s law (Moore, 1965) – the basic roots of the IoT paradigm is the availability to send data from one point to another over a network of some sort. Being able to send data from various objects is the key factor here, and that is why IoT was developed in the Auto-ID department. The key factor is the role that network technologies have; they have risen to be the main source of communication and can therefore take the challenge of having information and communication systems embedded in the environment among us (Gubbi, 2013). Radio Frequency Identification (RFID) is more than just a barcode on steroids (Ashton, 2009) as this has previously been the main source of communication in these systems. As history shows we have in the latter years seen technologies like Near Field Communication (NFC) which provides almost the same service as RFID, yet more technologically enhanced. Depending on what the IoT device sets out to accomplish RFID/NFC is still a valid choice, but today we have many other technologies to communicate autonomously between devices with, such as ZigBee, and IPv6 (Kovatsch, et al., 2010).

The IoT concept has the potential to change the world like the internet did, and maybe even more so. Due to innovation in areas such as networking, wireless technologies and IT technology in general the IoT paradigm is changing still, and therefore IoT will probably have a huge impact in the way the world works, as we know it (Ashton, 2009). IoT is defined various ways, most of which sound similar to the following definitions:

- *The network formed by things/objects having identities, virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate with the users, social and environmental contexts (EPOSS, 2008).*

- *IoT is going to create a world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these “smart objects” over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues (Haller, 2009).*

Google Trends show that the overall interest for the IoT phenomenon has grown a lot during the past few years, and even months.



1 - Google trend

The overall interest for the search criteria (Internet of Things, IoT, and IT Security) have increased, but what is most noteworthy is that the search term: “IoT” especially have increased from 2014 to 2016. The same goes for the blue line “Internet of Things”. The correlation between the red/blue curve (IoT) and the yellow curve (IT Security) as well as having the IoT phenomenon at its highest of the Gartner hype circle for emerging technologies (Gartner, 2015) allows for a report like this.

Due to the fact that we see an upwards trajectory in new trends like this, suggests that companies will have to take a stand on whether they want to adopt new technologies into their businesses. The incentive to adopt new trends like IoT into the business can obviously vary a lot from company to company. Some might have an economical incentive to increase productivity; others might want to allow their employees to use whatever devices and gadgets they feel like in order to allow their employees flexibility in their workflow. Some industries could potentially have other incentives to, not allow their employees to use any IoT enabled devices except company issued ones due to specific threats, issues or compatibility/partnership/image issues.

As we have seen in the latter years, Bring your own Device (BYOD) is a previous phenomenon that companies had to take a stand on whether they would comply with their employees desires to use their own products or not. As the innovation and general evolution of IT appliances continue, employees might find IoT enabled devices useful in their line of work, which forces the companies to find a solution for their business.

As IoT devices often are unmanaged and rarely updated devices makes it a risk to just allow in to the network. The allowance of various IoT products can therefore vary from company to company, in some organizations bringing in a specific device and putting it on the network can in some instances cause havoc and put the company network security at risk, whereas the same device in another organization is rather harmless for its environment. These different risk factors need to be understood by the leadership in the company in order for them to guide their employees, and align company and employee interest, for the best possible outcome. Having a leadership that allows IoT devices on a broad scale is not necessarily a good thing due to previously mentioned statements. Having a management that allows IoT devices within certain parameters in conjunction with IT technicians with sufficient knowledge about the overall IT infrastructure and network infrastructure is a key component of properly integrating IoT devices in the company.

In order to decide whether or not to allow certain IoT enabled devices, one must first understand the risks involved. Some of the potential risks is as follows:

- Exploit default passwords to send malicious spam emails.
- Exploit poor network configuration to steal personally identifiable information.
- Overload devices in order to render the devices inoperable.
- Interfering with business transactions.

This report sets out to make a set of guidelines that companies can apply to their own context, from a management point of view, in the area of overall IoT security. Due to the guidelines being directed at a management level, it is essential for the guidelines to incorporate eventual consequences from both a security but also a business strategy aspect. The guidelines will have to be rather non-technical as they are subject to be read by individuals that are not experts in the field, and in some cases in along with IT specialists. In order to create these guidelines the report includes the generic and tested standard ISO27001.

1.2 Statement of intent

The concept of IoT is rising and turning from being a phenomenon to a tangible thing for some companies and in the following years IoT will be a tangible thing for everyone (Uckelmann, 2011) – This enables the companies to not only improve productivity but also minimize costs and optimize processes, this however comes with a price.

The price of all these benefits is that IoT devices inherit many issues from them being small computers which mean that every single device is inheriting security issues that regular computers also experience (Uckelmann, 2011).

Due to the fact that not all companies are equal, their differences in size, goals, data handling, scalability etc. suggest that making a set of guidelines for companies to handle the threats IoT creates, has to be in the general sense. Even though companies will have to use an individual approach in order to tackle the issues, having IoT being brought into the companies creates various issues (Uckelmann, 2011). A set of guidelines should provide the company with the most essential measures to contain the most common security aspects that IoT brings with it.

In order to achieve the goal of creating a general set of guidelines with the potential for management to meet the security requirements, for their companies context some general IT standards will have to be taken into consideration. In order to do so the ISO 27001 Information Security Management standard will be providing general information in regard to various technology related issues that a company might have to address (ISO.org, 2013).

Due to ISO 27001 Series being one of the main 'Information Security Management' standards, the guidelines will touch upon the series and its compliance with IoT security issues and issues attached to other networks than the internet (Zhou, 2013). Comparing the ISO27001 with the findings in form of trends, objectives and obstacles (Andersen, 2006) from the literature about IoT security aspects, will be the foundation for a set of guidelines on information security management revolving around IoT. The information gathered is in a form of a literature review (Webster & Watson, 2002) this will create a knowledge base of the overall security obstacles and threats in which companies can encounter. In order to test whether or not these obstacles and threats are in fact purposefully suited for a set of IoT specific guidelines, the first iteration of guidelines will be tested by conducting interviews with experts in the field.

1.3 Problem Definition

Based on the statement of intent and the previously mentioned upwards trajectory in terms of the interest of IoT the following definition of problems is what this report sets out to explore.

How can companies handle security with the introduction of Internet of Things devices?

- What essential security issues does IoT bring into the companies?
- How and to what degree should companies handle these security issues?
- Which security issues does ISO27001 Standard comply with, in conjunction to IoT?

1.4 Delimitation

This reports goal is to disclose a set of guidelines with base in generic topics which every organization potentially can use directly or to raise awareness of potential pitfalls. During the process of creating the guidelines a set of limitations has been made in order to not extend the initial thoughts and ideas about the study.

The limitations made around IoT as a whole is that there is not described a specific device or solution which much of the literature does in order to conceptualize and make their readers understand the different values. However in this report IoT is only mentioned in a generic form, so it stays true to the effort of making the guidelines available for everyone to use.

The ISO27001 is used in order to secure the test of IoT falls into 'regular' it security measures. It is limited to only being the ISO27001 standard even though ISO has many other standards which potentially could be applicable on a report like this. Among others there is Network security part one to five, and cybersecurity. See appendix 1 for the full list.

The guidelines are limited in the sense that they are not fully applicable to any scenario, but an organization needs to evaluate their context and see whether or not they can use all points or just a few of the guidelines for their beneficial security gain.

Chapter 2 – Related research and theory

2.1 Related research

The following chapter explains the theory and related research that is the basis for the analysis in chapter 5. However the knowledge from this chapter is created according to the literature review in chapter 4. The literature review provides the link between the literature and how the essential parts and combinations of theories are found. This chapter will furthermore provide information based on

what challenges IoT Security has and what is missing from related guidelines in order to function in the space of IoT.

Most literature on the topic of IoT security mentions a specific type of device what describe its flaws. Furthermore the majority of the related research provides knowledge on how to perform example attacks on certain devices, or groups of devices; for example internet enabled cameras and NFC enabled devices, such as door locks. The amount of research papers with relation to a specific device type is rather large; and many of the articles are highly attached to a certain level of preliminary technological knowledge. Furthermore there is only a limited amount of research papers that include the topics: IoT Security, Network security and Management hereof.

Based on this observation it leads to believe that there is a gap in the literature that leads to this study in regard to finding a set of generic statements that can provide management level employees with the know-how to assess the risk and vulnerabilities involved with the type of IoT solution they seek to introduce into their organization.

2.2 Theory

The following segment will describe and explain theory from these topics, which are also based upon chapter 4's literature review:

IT Security, present an overall understanding of how IT Security works to protect Data and Services.

Internet of Things, will introduce the IoT Flower Model and provide knowledge into how IoT combines multiple aspects.

Standards, presents the ISO27001 and the PDCA model.

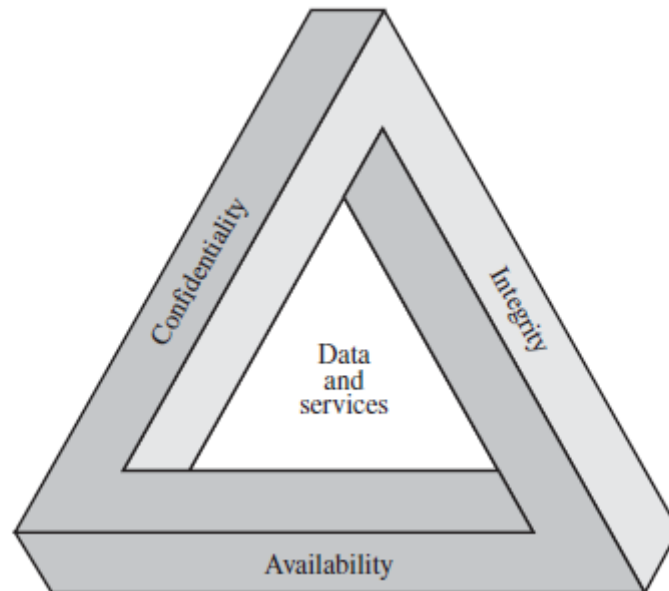
Risk, introduced six points by Pfleeger to optimize risk assessments.

Organizational processes and leadership, presents Marshall & McKay's key areas of important participants in a transformation process.

2.2.1 IT Security

The CIA (Confidentiality, Integrity, and Availability) model is an acknowledged model for General IT security (Matthew Haughn, 2014) (Pfleeger, 2015). Due to the fact that IoT is a compilation of a various amount of areas within the IT space, the security aspect is also very broad. Due to the overall

broadness of the IT Security in question, it is not useful to go into detail with for example SQL database security, but rather go into the overall aspect of how security can be obtained.



2 - CIA Model

The three components of the CIA model are the fundamental objectives for data and computing services.

Confidentiality

The term confidentiality covers two concepts namely Data confidentiality and Privacy which are set in place to limit access to information.

The data confidentiality concept assures that data is not made available for unauthorized personnel. Some of the methods used to ensure confidentiality are data encryption and user IDs, passwords and two-factor authentication. In special cases this might even include biometric verification methods and security tokens.

The privacy concept assures that the individuals with access to the data are authorized and educated in safeguarding the information they have control and viewing rights over. This aspect also ensures that only people with right authority have access to said files. This measure is helpful in social engineering cases since it can prevent uneducated people to leak information that they might not even need to have access to.

Integrity

Integrity is also divided into two concepts; Data Integrity and System Integrity. The integrity works around maintaining the consistency, accuracy and trustworthiness of data during its lifetime in the systems. Data integrity is to assure information and programs are only changed by intended changes made by authorized users. A few simple rules of thumb in this scenario are that data must not be changed in transit, and there must be a test on the data structure to see whether or not the data has been altered by unauthorized sources.

System integrity, much like data integrity, is to assure that the system performs as intended, without manipulation of the system from unintended and unauthorized users. Some of the most common technologies used to secure data are intact is checksums and cryptographic checksums as these show a binary evaluation of the data structure. Furthermore Backup and data redundancy must also be available in order to restore affected data to its initial state.

Availability

This point is to assure availability and that the system works properly within the given parameters for uptime and that no functions and services are denied to authorized users. So the essence of availability is that the systems and information are available to the users whenever they need them. The key aspects are to make sure that hardware requirements are met, and that hardware is maintained and repaired promptly in case of failure.

Besides the hardware aspect availability is also to make sure there is enough bandwidth, redundancy possibilities and disaster recovery procedures in place in order to secure uptime and availability.

Additional points

The three concepts of the triad provide an overall view of the objectives for IT security, yet some propose a few extensions to the model, which most commonly include Authenticity and Accountability. The Authenticity concepts purpose is to secure that, users are who they say they are, and having a way of verifying such information and furthermore secure input into the system is coming from a trusted source. The Accountability assures that it is possible to trace security breaches to the responsible. Systems should have a log or record of activities to allow forensic analysis in the case of breaches.

The most common challenges for the CIA Triad is big data due to the amount of data that needs to be safe guarded and kept available. This requires a large infrastructural availability, and especially if data sets are to be duplicated and stored geographically elsewhere. Big Data is not the only

challenge the CIA Triad has; IoT is also a challenge in the sense that most IoT devices go unpatched due to the nature of these devices. The sheer volume of IoT devices in conglomeration can potentially also endanger data and privacy claims, one IoT endpoint device might not be endangered for privacy issues, but if multiple devices are compromised and the data transmitted is analyzed the imminent threat is very real all of a sudden. Due to the nature of the Triad and the challenges it has in regard to IoT the possibilities for securing the IoT devices will be examined in the rest of this report.

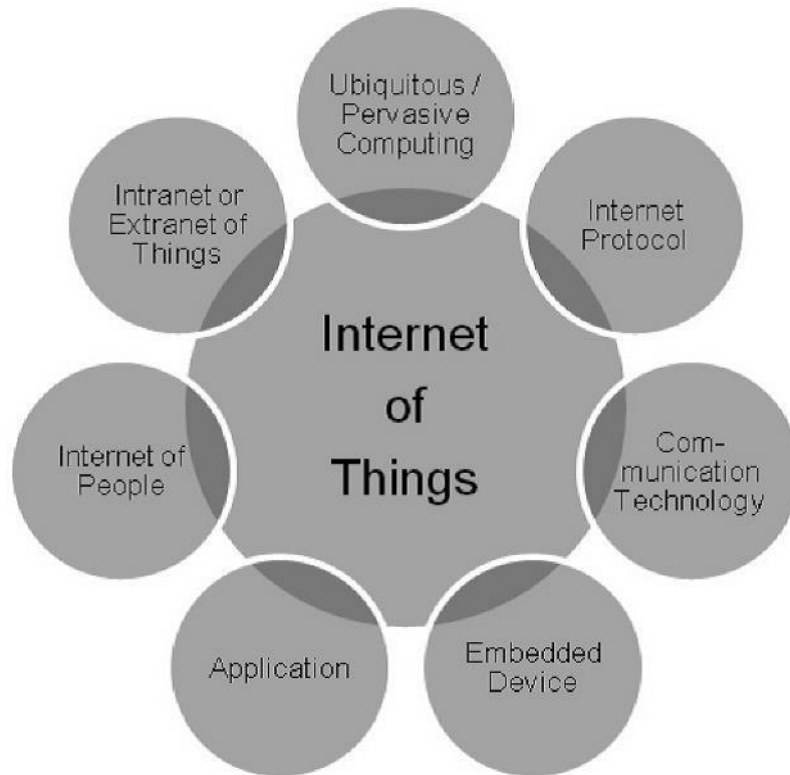
A comparison between attack methods and security technology can be seen in the following matrix.

Computer security attributes	Attack methods	Technology for internet security
Confidentiality	Eavesdropping, Hacking, Phishing, Denial of Service, IP Spoofing	Intrusion detection system, Firewall, Cryptography, Ipsec & SSL/SSH
Integrity	Viruses, Worms, Trojans, Eavesdropping, Denial of Service, IP Spoofing	Intrusion detection system, Firewall, anti-malware, SSL
Privacy	Spamming, Hacking, Denial of Service, Cookies	Intrusion detection system, Firewall, Anti-malware, Software, SSL
Availability	Denial of Service, spamming, System boot record infections	Intrusion detection system, Anti-Malware, Software, Firewall

3 - Daya 2013

2.2.2 IoT Flower model

The flower model is introduced by (Uckelmann, 2011) as a model of which all aspects sum up what Internet of Things consist of. In his efforts to obtain a model that shows how IoT is connected by many different things, Uckelmann coined most of the following topics from the CERP-IoT definition, and furthermore added detail that fits in to the description of every topic. The Flower model is to be seen as a model of the whole IoT space, and how things in that space connect and communicate with each other.



4 - IoT Flowermodel

Internet Protocol

Most new networking equipment supports IP v6, and the 128-bit addresses that translate into approximately 3.4×10^{38} addresses (S. Deering, 1998).

The IP Protocol is not the only way for IoT devices to communicate, there is a variety of ways since IoT is not under a certain “standard”. Some devices might use Bluetooth others might use another alternative radio for communication. As seen below, there are multiple protocols for connecting devices for home automation (Kovatsch, et al., 2010).

	X10	KNX	ZigBee	dS	IPv6
Medium	PLC, RF 310MHz (US), 433MHz (EU)	TP, RF 868MHz	RF 2.4GHz, 868MHz (EU), 915MHz (US)	PLC	Ethernet, Wi-Fi, RF 2.4GHz
Network size	2^8	2^{16}	2^{16}	2^{16}	2^{64} per subnet
Data rate	20b/s	9.6kb/s	20..250kb/s	200b/s	250kb/s..1Gb/s
Interface	custom solutions	application level gateway	application level gateway	Web services	UDP, TCP, RESTful Web
Maturity	1975	2002 (1990)	2004	2010	1998 (1969)
Costs	low	high	medium	medium	low
Installation overhead	low	high	low	medium	low
Connectivity	low	medium	medium	medium	high
Security	none	high (EIBsec)	medium (AES)	low (private circuits)	medium (6LoWPAN AES only)

5 - IoT Transfer mediums

As seen in the figure, there are many ways of transmitting data to and from a device, the key point of the figure is that we see there are little to no correlation between the mediums, which also means that they are potentially exploitable in multiple ways each and every one of them (Uckelmann, 2011).

Communication Technology – ZigBee, Bluetooth etc,

Communication technology in IoT is somewhat the same as when we talk about the internet. But in IoT it is not only HTTP, IP and Client/server structures. Some of the IoT technologies are more or less only used in that context, these technologies are mainly NFC and RFID but also the more low-tech QR code, which is a more advanced barcode.

Embedded Device

Embedded devices are devices that generally only run a special purpose computer program which is the function of the machine it is running on. Such devices could for example be routers, dishwashers, and ATM's. An embedded device can also be the actual tag from which the communication technology describes, RFID and NFC. These don't have any backbone structure which means that for these tags to work a set of criteria have to be enabled for anything to happen. Scanning a tag with a mobile phone for instance, the phone needs to have the Reader enabled, and it also needs an internet connection, if the tag wants it to open a URL for example (Uckelmann, 2011).

Application

The application is what is actually running on the IoT devices and/or people that interconnect and by being so, is the IoT phenomenon. The application is therefore a key component in any device.

“..the application, just as Google or Facebook could not be used in the early 90's to describe the possibilities offered by Internet or WWW” - (Uckelmann, 2011).

Internet of people

The internet of people term encompasses internet enabled personal electronic devices. This thing is spreading quickly in the consumer market as of today. Due to the ease and very low barrier of reaching people with smartphones with internet connections, and personal area networks these personalized items are working very well as a wearable for the human beings. An example of such wearables is the FitBit, which tracks heartrate and steps taken, but there is a lot of smart new innovation on this field, such as smart-clothing etc. (Uckelmann, 2011).

Intranet or Extranet of things

The internet is for everyone, and without specific knowledge you cannot know who anyone is, on the contrary to that there is the Intranet and the Extranet. The intranet is a closed network where everyone knows who everyone is within the business. The extranet is somewhat the same, but it scales out to a larger area, and it enables for example two firms to interconnect and have an extranet, (Uckelmann, 2011) where they can share large amounts of data or maybe a collaboration between firms in a brainstorming process.

Ubiquitous computing

Ubiquitous computing is in contrast to the normally used desktop computing where everyone has a pc on the desk, and that is where the computing power is used. Unlike desktop computing, ubiquitous computing can appear everywhere and anywhere, so it can be on any device in any format that you can think of. This topic is like an umbrella, which covers more research topics such as: Sensor Networks, Artificial intelligence, Location based computing, Context aware computing among others. (Uckelmann, 2011)

2.2.3 Standards

This section introduces the most common information security standard in most countries all over the world. The ISO27000 Series is a management tool that provides a set of a set of best practice recommendations on information security management. The standards vary from an overall set of best practice guidelines to a very detailed code of practice in specific areas such as Networking.

In this report, due to its nature and being directed against management level, there will in terms of ISO standards only be used the ISO27001 which is the 'Information Technology – Security techniques – Information Security Management Systems. This specific standard sets out to apply a list of controls the organizations that can be introduced to obtain a certain level of security.

ISO 27001

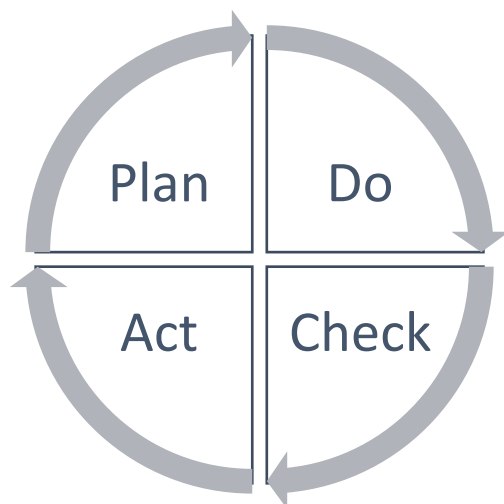
The ISO27001:2013 Standard is the latest revision of the standard from the international standard organization (ISO) (Digst.dk, 2015). This standard sets out to apply a very generic set of guidelines, which can apply for every organization no matter what. The starting point of the standard is to establish and implement the security measures and control procedures that apply to the organization in question. This standard emphasizes management involvement and how procedures and controls of said procedures should be implemented in order to achieve the best possible outcome.

The ISO27001 have a list of control parameters that should be sufficient for any organization in order to obtain a certain level of security. The Standard is very acknowledged due to its international nature which makes cross boarder collaboration and cooperation easy. Alongside the international acknowledgement the standard is also highly flexible which makes it compatible with other frameworks such as CoBit5 (A large business framework for governance and management of enterprise IT) (ISACA, 2016) and ISF standard of good practice (Forum, 2014).

The standardized “Best Practice” for information security in Denmark is to follow the combination of the ISO27001 and the legislation in the area. (Own interpretation of lecture, class: IT Governance, Revision, and Security) The ISO27002 is more technical, which is why only IT Heavy companies with the expertise to revise the standard should be using it (ISO.org, 2013).

PDCA Model

Due to the flexibility of the ISO27001 it enables the Plan, Do, Check, Act model (PDCA). The PDCA is a model for overviewing four different aspects of control and continual improvement in a specific organizational area as an iterative management method. The organizational areas could potentially be processes, production, but also information security management.



6 - PDCA Model

The four steps in the model each have its own function and are necessary for the model to continue in the iterations (Ronald Moen, u.d.). This model ensures structural procedures to review and examine information security risks. This model can be applied to any system, from both the individual practice and control up to the full implementation of an information security architecture and management system (Allen, 2006).

Plan: To specify what the overall goals are, within reason so it is possible to create a detailed specification of every aspect of the plan. Having a detailed plan enables for small scale testing for eventual outcomes.

Do: To implement the plan, whether it is to execute a process, create a product or implement IT security measures. Whilst implementing it is important to collect data for future analysis.

Check: This step is to analyze the implementation, adaption of what the initial plan essentially was. The results of the information gathered in the “Do” Step, these are subject to be compared against the expected results from the original Plan. Whether the analysis yields good or bad results it is, time to act upon them.

Act: If the check step shows whether the Plan step was implemented correctly during the Do step, and the analysis has yielded good results these results should be a new standard from the status quo (Allen, 2006). This means it is possible to move forward with a more optimized situation. If the analysis did not show an improvement the model suggests that you return to status quo, which obviously were the better solution given the results and try again with different parameters, therefore the iterative process (Ronald Moen, n.d.).

The PDCA model provides a structured procedure for the company to go through relevant considerations in regard to security risks.

2.2.4 Risk

Due to the nature of IT and how it works there will always be a risk involved in implementing an information system. Which is why a risk assessment should always be made when adopting new technologies or implementing new systems. This is also applicable when it comes to implementing IoT systems and/or devices. Risk assessments should prioritize business areas, which leads to involvement of the management of said the area in order to conduct an adequate risk assessment (Pfleeger, 2015). Involvement of employees with insight into the systems, such as operations managers are also required in order to minimize risk (Pfleeger, 2015).

The following six points are introduced by (Pfleeger, 2015).

1. Identify Assets.

By making sure all assets, data types and functions are identified and documented it is hard to lose track and miss something important.

2. Determine vulnerabilities

Depending on which implementation is made, it is important to determine vulnerabilities. In IoT this is also applicable, as for example patch management on IoT devices can be a vulnerability risk.

3. Estimate likelihood of exploitation

In any environment there will always be vulnerabilities which will be either easy or hard to exploit. Be sure to consider the differences between the pros and cons of each system.

4. Compute expected loss

An expected loss will depend on a variety of things, including the factor of the ability to respond to attacks and the consequences of successful attacks. This is often an indication of when smaller firms want to outsource some of the operations to experts in the area. For example outsource network operations to a provider which has the ability to monitor traffic etc.

5. Survey and select new controls

What adequate controls should be in place to maintain a high level of security and minimize eventual risk? Authentication and Access control, encryption, logging are some of the main topics when it comes to controls. Special environments might need other more specialized controls.

6. Project savings.

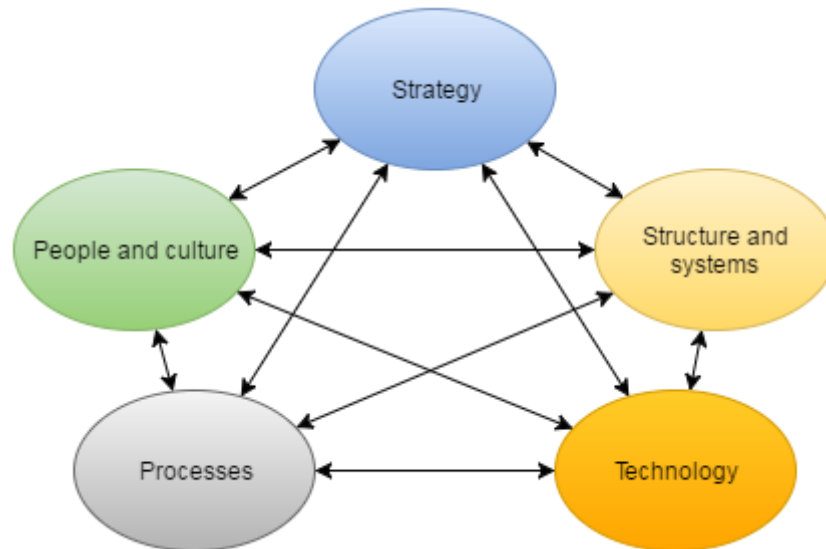
In regard to IoT implementations companies might estimate that they will be able to save an amount of money yearly due to improved production etc., via the IoT implementation. What most neglect to add into the calculation is that the system implemented might increase other posts, such as IT security controls.

Risk assessments are often only done once, which is a recipe for disaster these needs to be a continued process due to the fact that some risk change over time (Pfleeger, 2015). Some risk increases while others are lowering or even eliminated totally. The neglecting of the risk assessment process is often caused by the fact that the assessment is associated with an expense. One of the ways to lower the expense is to estimate what the cost of an implementation versus the benefit of having the control parameters in place.

2.2.5 Organization processes and Leadership

IoT can potentially have an impact on most areas of an organization depending on how and what kind of IoT devices and systems are implemented. This means that all employees and management

will have to interact with the IoT phenomenon in some way or another. A transformation as such can be put into a framework such as the McKay and Marshall framework for organizational transformation (Marshall & McKay, 2004)



7 - McKay & Marshall

This model indicates the various participants in an organizational transformation, and hereby enlightens the key areas of focus when implementing Internet of things systems and devices in an organization.

Strategy

The strategy is to establish vision and mission that will support and engage long-term success. In order for IT investments to make sense and create value for an organization it is essential that the investment is in alignment with the strategy, and hereby the vision and the mission of the company. Furthermore if there is no correlation between the organization's needs and capabilities an IT investment might not add any value to the company but rather just be a financial outlet. Strategy and IT Strategy is two different things, but these should have a correlation. There has to be a correlation due to IT only being a support mechanism for most companies, yet IT can support the overall strategy and potentially be involved in new processes and workflows that can increase the long-term success criteria for the organization as a whole. (Marshall & McKay, 2004)

Structure and systems

Company structures and systems indicate responsibilities and accountabilities of the organization, which is why they are often tightly knitted with the overall strategy. Organizational structure and systems are a vital component in implementing a strategy hence it allows for communication and

knowledge sharing which ultimately provide the optimal solution to customers and work partners. A dysfunctional structure and systems on the other hand do exactly the opposite and thus not engage in long-term success. (Marshall & McKay, 2004)

Technology

This part is pivotal in most organizations this day in age. The technology is slowly changing from a support role to a more integrated part of the companies. Due to technology being a more and more integrated part of the companies it also enables key business processes such as automation and support for employees in all areas of the company. It is important that the technology is driven by business objectives and requirements in order for IT to support organizational goals and change initiatives. In order to achieve the optimized use of IT capabilities it is essential for the organization to develop a strong partnership between the IT department and executives as this can provide innovation and improved processes. (Marshall & McKay, 2004)

Processes

Processes in an organization are ultimately to fulfil a request by either an internal or an external customer. Processes is a key aspect in how the product is being delivered to said customer, this is why it is pivotal in the strategic vision as you want to achieve the most effective and efficient processes.

Organizational processes can be enabled by IT investments as we see new technologies emerge all the time, this is why organizations need to be involved with innovation and have a deep understanding of workflow and processes in order to output previously mentioned efficient and effective processes, hence value for the company. (Marshall & McKay, 2004)

People and culture

In turbulent business environment transformations it is often necessary, but it is often hard to motivate employees to engage in a transformation with motivation and willingness. (Marshall & McKay, 2004)

People and culture is an essential part of the organization, those who feel motivated and empowered often succeed in their job which is why this part of the model is so essential. In order to empower and motivate people into a new process or workflow the organization can implement corporate reward systems and incentive programs to ensure everyone is allowing for changes to happen. The desired outcome of a transformation might also be achieved by changing management structure and administration in the process. (Marshall & McKay, 2004)

The previous part of chapter 2 shows the essential theories that will be used to create the set of guidelines, which will be tested in chapter 5.

2.3 Conceptual Framework

This paragraph shows how I conceptualize the theories around security, IoT, standards, risk and organizational structure and leadership in the context of creating a set of guidelines that can provide organizations with an insight into the threats and potential problems, that might occur in working with IoT. In order to attempt to secure the organization from potential IoT threats, one must first know exactly what IoT really consist of, its requirements and how it ensemble the various aspects of the organization it touches upon.



8 - Conceptualization

2.3.1 Security

Security is many things such as network security, system security and so on. In the following analysis, I will focus the “security” aspect around the CIA model previously mentioned, alongside the topics that the literature mentioned to be key areas as cryptography, access control, privacy, data handling and networking. Due to the abstract nature of the CIA model and how it can be used in any circumstance, I will use same objective view on the other theories in security, as they are all to fit into different scenarios in order to be eligible for the guidelines.

2.3.2 Internet of things

The internet of things theories is divided into two aspects namely architecture and the IoT Flower model. The way I conceptualize the information gathered from the theories is what kind of interfaces are important in certain scenarios from the architectural part of the theories. The IoT Flower model introduces the rest of the aspects in order to conceptualize what IoT consist of. The way this is going to be used in the analysis is to show how all these things interconnect in certain scenarios and how the various security steps overlaps and potentially provides an overview, of what security measures that are important in multiple given IoT systems.

2.3.3 Standards

The standards part of the theories is split in two, the ISO27001 standard which I want to use in order to see whether the previously mentioned IoT specific topics and scenarios overlap, with not only the chosen security topics but also the “mainstream” topics of ISO 27001 Standard.

Besides the ISO 27001 standard I will be using the Plan, Do, Change, Act model which allows me to provide the end product of guidelines with a perspective of an iterative process since most implementations concerning security in general requires controls in continuity and upkeep in order to stay relevant.

2.3.4 Risks

Pfleeger’s six points on risk and how organizations should interact with IoT in collaboration with risk is going to be the link between the more technical related topics of the Conceptualization figure and the Organizational structure and leadership aspect. The reason for introducing risk assessment into this report is in order to secure that the overall statement of intent from the set of guidelines is to bring every aspect of the organizational infrastructure in play when considering using IoT solutions. Risk is inevitably a large part of any form of investment whether it is financial or an investment into IT systems.

2.3.5 Organizational structure and leadership

The McKay and Marshall model introduce how IoT has an impact on all organizational structure and leadership in form of strategy, culture and people, processes, structure and systems and technology. All these topics from the model have overlaps in the previously mentioned topics from the other theory aspects of this report. This is why this model conclusively gathers all aspects of what should be included in the guidelines in terms of organizational transformation and points to be aware of.

2.3.6 Conclusive remarks

In the previous topics of conceptualization, it was stated how the theory is to be used in the effort to create the set of generic guidelines. As the previous paragraphs state many of the theories overlaps and can potentially be interconnected, the overall collection of theories should be sufficient in order to test out whether the hypotheses obtained from the literature are within reason.

In the five conceptualization points, it is furthermore described that there is a depth to every aspect in which a given context needs to be in place for the theories to function properly. Besides the context I also describe that some of the topics have a lot of subtopics which eventually can be essential in different scenarios for a given organization. Yet since the theoretical aspect is top to bottom and not in-depth in every aspect of it, this is due to the goal of creating a set of guidelines

and thinking points that should yield the user of the guidelines to consider and reflect over hitherto unknown or unfamiliar issues for their specific given context.

2.4 Guidelines and challenges for security

There are various types of guidelines in form of security in IT. As mentioned previously the ISO27001 standard is a general information security management which is one of the main information security management tools. ISO has many guidelines in terms of various technology aspects, such as networking, storage and financial services. However they have yet to create an IoT specific standard, which also allows for a study to create a set of guidelines that cover the challenges IoT has in terms of security. The ISO27001 together with the CIA Model produces a solid foundation of knowhow into what is essential to 'secure' in order to maintain system uptime in relation to regular IT solutions. There is however a lot of challenges with IoT in the sense that this new form of the landscape in the organization infrastructure provide various types of potential threats.

Some of the most common challenges brought into the organizations due to IoT is that the IoT devices often inherits the security vulnerabilities from the PCs due to the IoT devices essentially being a small computer device (Uckelmann, 2011). Due to that fact some of the challenges that IoT face is similar to regular IT security measures. However IoT does also introduce a set of specific threats to its environment.

The largest challenges for security in closer relation to IoT are however often addressed in the literature as being an architectural problem. Most devices are created without security in the design phase (Uckelmann, 2011) which results in poor configuration abilities and bad management capabilities. The bad management capabilities force organizations to consider the possibility of a huge increase in unknown vulnerabilities at the device level, due to the lack of antivirus or advanced threat detection capabilities (Cisco, 2015). Furthermore the lack of architectural standards increase the possibilities of exposed API's, and poorly manufactured low powered hardware solutions which lower the possibility of up-to-date encryption methods. Poorly configured devices increase the potential challenge of securing personally identifiable information and with our lives becoming more and more digitalized this is a huge challenge for the IoT space.

To summarize, there is a lot of challenges regarding IoT which not only has its ground in the inheritance from regular IT devices and systems. Due to IoT bringing so many devices into the

network it is essential for guidelines to purposefully explain how and when to harden the security measures tailored to IoT in order to minimize risk

Chapter 2 introduced the gaps in the literature study and presented the main theories that will be used to conduct the analysis. Chapter 2 also introduced the main guidelines that will be used, and the challenges that security have in this context.

Chapter 3 – Methodology

In this chapter, the method used in order to answer the questions in the problem definition will be introduced. The chapter will show the approach taken to find relevant literature and show how the collection process of empirical data is done. The last part of the chapter will present the scientific positioning as well as a discussion on the validity and reliability of the literature and empirical data presented.

3.1 Approach

In order to achieve the best possible selection of literature I have used multiple sources to find academic literature on the various subjects that intertwine in the report. The primary source is via the CBS library, and their online tool *libsearch*. The secondary source for acquiring literature is *Google Scholar*, which provides the same type of material as the primary source. Besides the two search engines I have acquired books and other academic literature from my studies at CBS, in classes like IT Security, Internet of Things and Organizational and financed focused courses. Furthermore I acquired articles on information technology security from colleagues at the CBS IT department.

In order to answer the questions in the problem definition I systematically went through articles that I had already read from the security and IoT courses which had previously been attended, this was done in order to create an overview of the most important aspects of each course. Having an overview of the essential parts of the two key courses, I set out to find literature that complemented what I had already read, to broaden the knowledge that I had acquired. The more I read the more new topics came up which lead to more new literature which had the overall topic of IoT and security. In order to systemize all the literature I created a matrix with takeaways from each author, see Appendix 2 for the snippet.

The Matrix works as a reading guide as well as an overview of what literature contains what kind of information, on the desired topics for the report. To create the first initial set of guidelines the matrix was a source of the authors that had mentioned certain topics as special for IoT Security.

In order to create the literature review (which can be seen in chapter 4) the reading matrix was the main source of how to conduct it. The literature review is created in a concept-centric way which is built upon a concept matrix (Webster & Watson, 2002) that has been created by reading the material in the reading matrix.

The concept-centric arrangement summarizes the concepts fully in the sense that every concept is isolated instead of using the article-by-article approach which I felt go more in depth in to the article instead of the overall concepts. The finalized concept matrix is used to create the first set of guidelines in the way that every time a concept is mentioned increases the way it is applicable to the IoT security guidelines.

3.2 Empiricism

Even though IoT is a relatively new concept, there is a lot of academic material on the subject. Most of which have its roots based on various devices, or device types. The literature used for this report is on the other hand more generic in the sense that it touches upon security aspects as a whole with a focus on the IoT concept.

The literature provides various sets of observations, which can be used to generate a set of guidelines that provide companies a structured way of allowing their employees to use IoT devices within the work environment, in a secure manner. This set of guidelines is subject for a test to see whether it works in a real work environment.

In order to test the guidelines and theory accustomed with the guidelines I have conducted semi-structured interviews with industry experts.

The initial communication with the experts was over mail, as this provides certain flexibility in regard to initializing contact and planning of interviews. Due to mail not being the best medium for explaining and talking about technicalities, it was only used for small messages and clarifications of questions for the interviews.

The agreements with the individuals which agreed to operate as interviewee were that they agreed to meet and engage in an interview, initially talk preliminary about their knowledge on the area to

establish the expert role. Furthermore a more in depth interview which is based on the theories gathered on the topic.

The semi-structured way of interviewing was chosen before meeting the interviewees and an interview guide had been conducted beforehand as well, (Appendix 3) this allows for the interviewee to use their own experiences and knowledge into the answers given. Furthermore it also allows the interviewee to explain a certain situation which potentially lies outside the boarder of my own knowledge on the area.

By conducting the interviews this way it was ensured that the answers are given where the interviewee's own, as I did not force any specific theories and/or thoughts into the answers.

The semi-structured interviews also allowed to change up the questions as the interviewee kept talking from one, the question to another. This allowed the interviews to be more of a talk than a questionnaire type of knowledge gathering.

Due to the interviewees being Danish, the interviews were conducted in Danish which potentially can bring forth implied answers in the sense that the questions were very close related to previous ones or that the interviewee kept going in the direction of their train of thought based on the initial questions. Having the interviews in Danish means that sentences used later on in this report have been translated into English. This can ultimately also cause a small interference in the understanding of the questions, but since most of the answers is somewhat black or white and most content surrounding the security topics is mostly English words as well, it is not considered to be a massive disruption to the outcome of the interviews.

The interviewees all wanted to be anonymous as in they do not want their names used in the report, however one allowed for the company name to be admitted, he works for Mærsk, the other only title of the job description which is IT security teacher.

3.3 Validity and reliability

The validity touches upon the gathered data is relevant in the specific context it is used. This is why I used a vast amount of time digging for relevant information in both articles and books regarding not only Internet of Things but also security and organizational structure as a whole. This data gathering and analysis has been an iterative process as one theory leads to another, and due to the subject complexity many theories melt together in the broader scheme of things as IT Security has its roots

in many other areas such as psychology, networking, manufacturing, management, and governance. Due to the iterative process I ensured that the theories I found interesting had a connection to the problem definition, but allowed for deviation in order to secure the validity of collected data.

The reliability is about the sources and data collected is reliable in the context it is used. As previously mentioned the overall topic of this report is broad in itself as it contains multiple subjects, I have chosen to investigate every topic in order to get a knowledgebase that can emphasize that the areas I wanted to focus on were the correct ones. Many articles have their roots in certain IoT devices and/or theoretical works which have provided me with a subjective understanding of the different areas of the subject. Choosing such articles promote the reliability in the form that the study potentially can be done at another time by another person and end up with the same conclusions.

The reliability of the data collected from experts has a few drawbacks in the sense that whenever you interview a person, there is a chance that they might give untrue statements. In this case I do not feel that is the case, due to the fact that I have had little to none interactions with the interviewees and they have large amounts of experience in the field.

As far as the scientific theories go the reliability is somewhat limited in the sense that I have not had any chance to interview all types of organizations and experts. In order to make up for that I have gotten information from experts from different areas of expertise in the field of IT Security.

3.4 Scientific positioning

The scientific positioning chosen for this report is primarily the inductive method, this approach is a scientific method that achieves having empirical observations generalized into a few powerful statements that show how the environment, in which the study is made, works. (Kuhn, 1977)

This theory does have some scientific issues though one of which is the limitation that it is only possible to conclusions based on what observations there is made. An example hereof could be:

It is observed that the steering wheel is placed on the left hand side of the car.

Conclusion: All cars have the steering wheel on the left hand side.

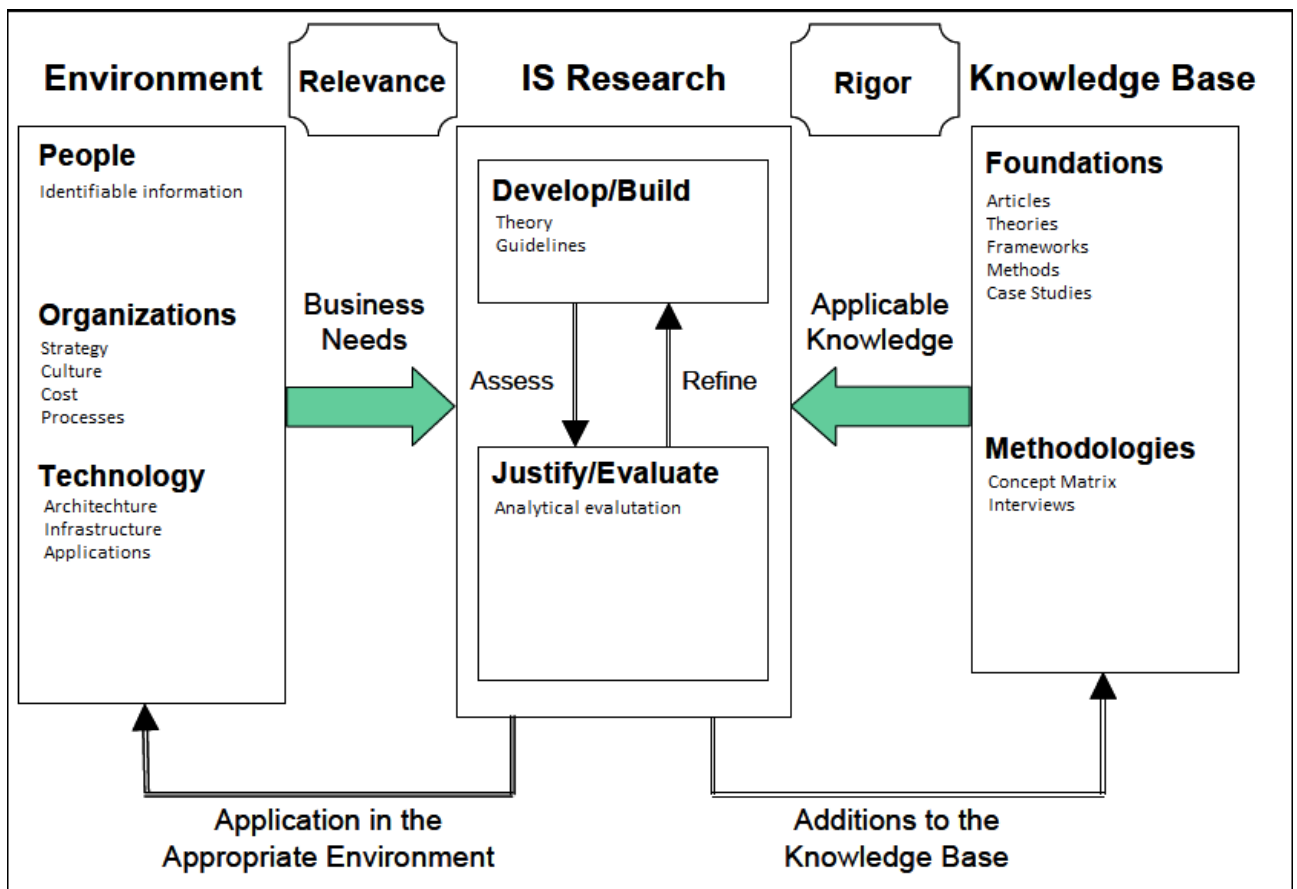
This is not the general truth though, as we, all know that England among others has the steering wheel on the opposite side of the car. This shows that the inductive method has some limitations in

regard to what observations there is made. The following statement can explain the limitation of the inductive method: “You can only see what you are looking for” (Kuhn, 1977).



9 - Inductive

As the model shows, the inductive part starts with an analysis of literature that provides the observations of what the literature says is most important. This gives a certain degree of knowledge in order to create a hypothesis that what the literature says is correct. In order to test whether the findings in the literature is indeed correct the findings will be used in a set of interviews to find out whether or not the experts agree with the literature findings. By creating the guidelines like so, it points towards Design Science, which is why the following model is included.



10 - Design science

This model by (Hevner, et al., 2004) shows how the framework tailored for design science research, in the boxes there is stated what applicable topics is used in this report in regard to the framework.

Hevner describes seven guidelines for an understanding and finalizing research within the design science research parameters. These seven guidelines are subject to find problems in areas that might not have been considered and by running in iterations ultimately eliminate these problems.

Due to the roots of the inductive methodology mentioned in the beginning of this paragraph and the quote “You can only see what you are looking for” (Kuhn, 1977) the inductive method would limit the research, which is why the design science framework is included.

The design science framework allows to reiterate and build the knowledge base by using the seven-step guideline (Hevner, et al., 2004). Ultimately the framework allows for the guidelines to impact the environment, in which the research is conducted.

Chapter 3 presented the approach to data collection alongside where and how data is found. Furthermore it also shows how data is collected and being used, in terms of interviews. The last part of chapter 3 shows how the validity and reliability of the report are constructed as well as the scientific positioning between inductive methodology and design science framework.

Chapter 4 Literature review

As mentioned in the methodology chapter, the literature review is mainly based on the Webster and Watson, 2002 article and it is arranged in a concept-centric way, so each concept is being thoroughly handled. The focus of the literature review is to outline essential parts of literature in regard to IoT security and what it consist of. The following concept matrix is based upon the reading matrix which can be seen in appendix 2. The concept matrix will show how the literature positions the key concepts.

The key concepts, those with a larger amount of mentioning are standalone but as there are multiple concepts that intertwine one way or another in the Concept Matrix, these have been concatenated in the literature review in order to justify the concepts by theoretical explanations, past empirical findings, and practical examples (Webster & Watson, 2002).

Due to the fact that IS security is underlying IoT security in many ways these are concatenated, further more is data transfer included in data handling as these also are very similar in their conclusions regarding IoT.

Articles	Concepts								
	Data Handling	Architecture	Network	Privacy	IoT Security	IS Security	Data Transfer	Cryptography	Access Control
1	1								
2		1			1				
3	1	1	1	1		1	1	1	1
4		1							
5		1			1				
6	1			1	1				
7				1	1				
8		1	1		1	1			
9	1	1	1		1				
10		1	1	1	1		1	1	1
11	1	1	1		1				
12	1	1	1		1				
13		1	1	1	1	1			
14		1	1	1	1		1		1
15			1	1	1				1
16	1	1	1		1	1	1	1	1
17		1	1						
18		1	1		1				
19	1	1	1		1				
20	1	1							
21	1	1					1	1	
22		1	1			1	1	1	
23			1	1	1	1	1	1	1
24		1	1		1	1		1	1
25	1	1	1	1	1	1	1	1	1
26	1	1							
27	1	1	1	1	1				
28			1	1		1		1	1
29		1							
30			1						
31	1	1	1	1	1	1	1	1	1
32	1	1		1	1				
33		1	1	1				1	1
34			1		1				1
35		1			1				1
36				1				1	
37					1				
38			1	1					1
39					1				
40		1			1				
41		1			1				
SUM	15	28	24	16	27	10	9	12	14

11 - Concept Matrix

4.1 Architecture & IoT security:

Architecture and IoT security is a very broad concept, yet they are interconnected in such a way that they rely on each other for a very large portion of the literature. Architecture is seen as an umbrella term, as it covers over a lot of different types of architecture types. Many of these terms is technical, in the sense that for example business IoT architecture (Haller, et al., 2010), communication architecture (Kovatsch, et al., 2010; Giusto, et al., 2010) and middleware architecture is mentioned (Atzori, et al., 2010; Alsaadi & Tubaishat, 2015; Giusto, et al., 2010). The idea of IoT being divided into various architectural groups is agreed upon it is said that IoT is a three-layered architecture with Sensor Layer, Network Layer, and Application layer (Zhou, 2013).

However as a whole it is said that IoT does not have a standard architecture yet, (Jing, et al., 2014) this statement is replicated in multiple articles regarding overall architecture and left out in articles with specific technological architecture types.

IoT security is inheriting the issues from regular IS systems (Uckelmann, 2011) due to its nature of the devices being essentially a small computer. It is mentioned that IoT consists of three layers, namely the perception, transportation and application layer (Jing, et al., 2014), each of these layers have ties to the other concepts in the literature review. IoT networks need to be worried about both sophisticated targeted attacks from competitors and nation-states, as well as accidental misuse from employees, contractors, and vendors (Cisco, 2015). IoT devices are often remote devices which make them less likely to be properly secured and managed (Alsaadi & Tubaishat, 2015). In order to properly secure and manage the IoT devices it is mainly said that the devices need to have the resilience to attacks, data authentication, access control and privacy measures (Weber, 2010; Jing, et al., 2014; Maras, 2015). Private enterprises using IoT technology should therefore include these requirements into risk management (Weber, 2010).

4.2 Data handling:

The literature states that most of IoT solution and devices are accompanied with wireless technologies in one way or another. It is mentioned that in the IoT space that data is not only useful when it is locally applied, but the usefulness increases tenfold when it is connected to multiple sources such as databases (Rowland, 2015). Rowland continues to say that the raw data does have a low value, but if the data handlers are able to extract the meaning of the raw data, it is possible to generate actionable insight into the data and use it within the context. Both the internal and external network is essential in order to create value and effect of the data collected (Qiu, et al.,

2012). Qiu continues to state that data flooding is a very attractive way of attacking IoT solutions due to the way the devices handle data and the devices easily being bottlenecked.

It is mentioned that one of the most important areas of emergent technologies like IoT is to create an unprecedented amount of data (Gubbi, 2013). As there is a continuing increase in the use of cloud based analytics and visualization platforms it is foreseen that this increase indeed will be used more in conjunction with IoT (Gubbi, 2013).

4.3 Network:

Network security is one of the greatest challenges of IoT. IoT is a three-layered architecture with Sensor Layer, Network Layer, and Application layer (Zhou, 2013). The network layer is in the middle of the two others, which is why it is an essential part of IoT. In the network layer is Routing and Addressing placed, which is two of the main issues with IoT networking (Giusto, et al., 2010).

The sensor level is also known as a wireless sensor network (WSN) which is a dangerous environment due to its open and often unattended way of being a transportation medium for data (Meghanathan, et al., 2010). The low cost of sensor nodes in a WSN is subject to hinder data authentication and that some methods of cryptography and authentication only solves some of the problems WSN's encounter (Meghanathan, et al., 2010).

In order to traditionally secure the network as for IoT a list of various terms is being mentioned again and again. The following five topics are allegedly really important when we focus on IoT networking: Access, Confidentiality, Authentication, Integrity and non-repudiation (Daya, 2013). Many others mentioned these topics, however the most notable use of these is in combination with the CIA triad (Stallings & Brown, 2012) which is a general model for securing services and data within the network.

A Mapping of each network asset identifies a logical network segment that allows subnets to be evaluated and clearly identified. A clear identification of subnets allows for evaluation of the various subnets in terms of criticality, access requirements/access control, and other security measures such as firewall zones between the segments (Shinder, 2005; Daya, 2013; Pfleeger, 2015).

4.4 Privacy:

In IoT Privacy an abstract problem that requires attention from both manufacturers but also users of IoT solutions and devices (Maras, 2015; Uckelmann, 2011). Due to most IoT devices having sensors, privacy is an essential part of the security aspect of the devices. The IoT privacy concerns are shared

by many, it is also mentioned that enterprises using IoT technology should include client privacy into their risk management concepts (Weber, 2010). Weber furthermore includes some privacy enhancing tools, which can be beneficial in order to secure privacy for using IoT technologies.

It is mentioned that the part of computer security that often is left out is privacy (Stallings & Brown, 2012). In that statement it is further mentioned that the emphasis is on the scale of interconnectedness personal information which is being increasingly collected in the world we live in today (Stallings & Brown, 2012).

(Weber, 2010) also includes a paragraph on a legal course of action in relation to IoT technology. The paragraph shows how the European commission has guidelines to how member states can provide guidance with respect to privacy concerns. This trend is continued as (Stallings & Brown, 2012) continue to talk about the European Union and others like the United States that have guidance and legislation in place for its member states, when it comes to securing privacy of its citizens.

(Stallings & Brown, 2012) mentions the rights for the users whenever their data is collected, and furthermore they advise that the ISO27001 policy should be communicated to all persons involved with processing person data.

4.5 Cryptography

In relation to cryptography IoT has a few troubling aspects, the main one being that most devices are primarily low powered devices which make them unable to handle encryption levels of a certain standard and thereby leave out cryptography which is essential to prevent eavesdropping from external network devices (Atzori, et al., 2010). It is mentioned that the primary communication method with IoT devices is on IP based networks (Xu & Perakovic, 2016) it is also mentioned that the state of most IoT data transmission problems is resolved by applying cryptography standards (Xu & Perakovic, 2016).

Cryptography in its most plain form requires computing power in one way or another in order (Stallings & Brown, 2012) to secure that the encryption and decryption of cipher text, and running the algorithms in a timely manner. The most secure methods of encryption are increasingly requiring more compute power in order to function within certain time parameters which are why low powered devices can be potentially too slow to encrypt and decrypt and hereby create a bottleneck with the data transfers (Stallings & Brown, 2012; Pflieger, 2015).

There is an emphasis on how cryptography can be hard to use on certain systems as he states that RFID tags and cryptography is still prohibitive as it often violates application requirements such as power (Giusto, et al., 2010).

The cryptography aspect requires power dedicated to the devices in order to function well enough to be useful in the long-run (Pfleeger, 2015), and as the literature states it is worthwhile having encrypted data transmitted so eavesdropping and other methods of obtaining data from the network is minimized to the least possible potential of data theft (Stallings & Brown, 2012).

4.6 Access control:

In the effort to restraint access to the IoT devices, it is stated that in especially production environments it is very critical to ensure access control to the devices (Uckelmann, 2011). This is important due to having the ability to ensure logging and that the devices, are not tampered with in any way shape or form.

IoT is often unattended and unmanaged devices, which make them easy to physically or remotely gain access to (Atzori, et al., 2010). Other articles also talk about the physical barriers for devices connected to a network segment. In that context (Meghanathan, et al., 2010) states that a device needs one or more physical objects to be crossed in order to achieve access to the device in question. Furthermore (Meghanathan, et al., 2010) also says that remote access is a reliability as devices on a network is required to have password authentication and logging on device configurations and login attempts from a remote location.

(Uckelmann, 2011) States under the chapter of costs of the internet of things, security and networking are positioned at level six of seven. Yet they stress that security and access control both physical and remotely should be invested in, in an enterprise environment of IoT.

Access control needs to be controlled by those who provide information to the system and hereby also control the accessibility to the data (Weber, 2010).

In terms of access control (Stallings & Brown, 2012; Pfleeger, 2015) mention the overall security aspect of access control, where authentication, authorization and audit is in focus for most typical systems. They continue to stress what various ways of securing access control primarily remotely, and the importance of having a combination of different access control policies. In their closing arguments of access control in systems related to network segments, which IoT definitely is, they utter the audit part again in relation to keeping the user accounts with access at a minimum, and

reviewing them frequently. The frequent review is mentioned to be a process to delete unused, or closed accounts so unauthorized use does not occur.

4.7 Literature review conclusion:

Most literature describes IoT security as being an extension of IT security as we know it, however there are key factors learned in the literature review which potentially can be key points in the analysis. The most noteworthy lessons learned from the literature is that IoT is not one singular thing when it comes to security, which the concept matrix also states. IoT security is all of the above, some more than others in special scenarios. During the literature review it was noted that architectural standards are a necessity according to many, however there are a lot of literature with roots in the communication architecture, but not the overall IoT architecture standards that only some authors talk about. I also learned that network requirements and network security are far from all when we talk about IoT security, which I initially thought. The other concepts such as privacy, cryptography and access control are also key points which a lot of the literature correctly point out. Some even point out that privacy is often let out of security talk and research which seem to be a huge mistake. This even more so this day in age, where we collect so many data and a lot of that data actually invades the privacy of for example employees, one way or another.

Chapter 4 presented what concepts are most critical in order to secure IoT devices. The concepts will be used in the following chapter as I will take an analytical point of view on each concept mentioned in the literature review. These literature findings are supposed to create a base for the guidelines, which in combination with the theories mentioned in chapter 2 represents the first iteration of the guidelines. This first iteration is subject to be tested in the latter part of the following chapter when it is being analyzed with information from the expert interviews.

Chapter 5 Analysis and test of results

The reasoning behind attempting to create a set of guidelines instead of demanding exact requirements is due to the desire of creating a product that can be used no matter what company size, budget or even strategical goals that are. Guidelines are a great way of providing a tool of the generic recommendations that the organizations can use in their own specific context and thereby raise awareness around topics that might have been overlooked in previous attempts to create a secure environment. The essential thing is to create a tool that can be the baseline for organizations to control and consider certain topics which are important and necessary to secure quality and security of their information systems, and potentially productivity systems.

The analysis is based upon the literature and standards found on the IoT security topic, all the information that sprung from the literature are subject to be tested against expert knowledge on the field. This is done in order to see whether the literature used is actually as important as it proclaims to be.

Most of the IoT-specific literature focus on specific devices which renders somewhat useless in the sense that the guidelines need to be generic for all to use. The rest of the IoT-specific literature points towards regular IT security measures, due to IoT being such a diverse technology it links and connects many of the 'regular' security topics. By including all the regular security topics pointed to by the IoT literature I suggest that the results can be weighed against IoT security and explain the baseline of what level of knowledge and expertise is needed in order to implement IoT into the organization with a favorable level of security.

5.1 Analytic structure

In this paragraph the analytical model will be outlined and explained, this is used as the structure of the upcoming analysis that will be used to conduct and formulate the guidelines. As mentioned the goal is for the guidelines to be generic, which is why I am going to be using a generic organizational structure model. This provides a structured approach in the effort to identify how IoT affects the various areas of the organization.

Since IoT is not only a technology that is being implemented but rather a concept that can impact every aspect of the organization it is in some contexts worth looking at as a business strategy (Gubbi, 2013). This is why it would be wrong to only talk about IoT as a part of the technological infrastructure of the company and if there is no correlation between the technological infrastructure, processes and the people that need to be accompanying IoT it is hard to expect business growth or financial profit (Gubbi, 2013). This means that in the case of IoT implementations, multiple areas of the organization needs to be involved in handling responsibilities and controls in order to secure a healthy approach in using the new type of technology to its full potential.

As the literature clearly states the need for transparency between the organization and IT should be in place in order to leverage the full potential of the IoT technologies. This combined with the fact that the guidelines need to be generic in order for everyone to use them; there will be applied organizational theories on top of the technological ones for the whole concept to be valid for organizations to use them. This is the reasoning behind choosing to use the McKay & Marshall

transformation framework as a tool to put the conceptual framework into the context of an organization. This model is rooted in transformation and it is used to enhance the parts of the organization that is affected during a transformation process. I feel this is an important step to take in the context of IoT implementations and security around the implemented devices, in the matter that IoT impacts all areas of the organization and not just only a single department.

Even though a company only invest in an IoT enabled camera for the surveillance purposes, multiple departments of the company needs to be involved. IT most likely has security policies, and they are the ones having this new thing connected to their network which is the interface for potential connectivity to other areas of the companies' infrastructure. Investing in IoT devices like so requires leadership and management to delegate where the cost and man-hours for IT to service and secure the devices comes from. In a simple example as this we clearly see that IoT quickly can impact many areas just by acquiring a simple device.

During the first part of the analysis the essential parts covered by the theory in relation to the IoT context will be covered. During this analytical part the essential security issues IoT bring into the company should emerge. Furthermore these issues and aspects of security are then to be analyzed in order to objectify them into a business perspective.

5.2 Literature findings

During the material gathering of academic works on the topic at hand many sub topics emerged, and pointed out that they were essential in one way or another for the security of IoT systems.

As mentioned in the theoretical chapter, the topics that are introduced there stems from reading various articles on the topic of IoT security and their citations. This ultimately yielded a handful of topics that were indicated as essential for the matter of how most authors conceptualize IoT security and to what degree they see the subject fit in the context they are writing about. As an example, authors that write about big data IoT solutions have a higher emphasis on data handling than those that write articles on home automation.

To sum up, the theoretical points were as follows: *Architecture & IoT security, Data handling, Network, Privacy, Cryptography, and Access Control.*

I will now outline every one of these topics and mention the pros and cons concerning its affection on IoT security in the context of the business environment, which ultimately should allow me to

create statements that can be tested in the context of the conceptual framework in the next chapter of the analysis.

Architecture & IoT security

Due to the fact that this concept was somewhat of an umbrella for other categories and concepts it is limited with the takeaways. However the concept underlying IoT security is the following concepts, as has been learned in the literature review. In regard to architecture the common consensus is that there is no correct way of architecting the internet of things as this is written. Due to this fact, it is essential for companies investing in IoT technology to keep security a priority from day one. Security claims that vendors are making can't be validated by most organizations, due to lack of expertise in the area. The organizations with a lack of expertise hereof need external help or need to take the vendors word for it. Vendors need to provide evidence of security in devices, and if they do not provide evidence of that we need to assume that there is no security.

Data Handling

In extension to inference and privacy issues, the literature kept mentioning Data handling as a means of a potential security breach. When all IoT devices are accompanied with various sorts of wireless technologies it increases the possibility of security breaches as many of the technologies are easy to eavesdrop upon. As mentioned in the theory chapter, data is suddenly ten times more useful when it is connected to other data sources, which can increase the usefulness of the data as it is entitled to be compared and paired with other sources that ultimately seclude data which is designated useless, and improve data that suddenly is very useful as it is used in a larger context than the initial data gathering (Rowland, 2015).

Here we see the connectivity between data handling and the previously two mentioned, Cryptography and Privacy. Data Handling is essential in the matter that every other topic refers to it one way or another. The nature of IoT being devices with embedded identification, sensing and actuation capabilities, it is clear that the combination between the digital and physical entities are now linked in such a way that the infrastructure around the various devices needs to be the medium for securing a responsible approach towards introducing this technology on the more widespread basis.

Transmissions between point A and point B in any type of transmission scenario entitle most of the topics pointed out in the theoretical chapter, and in the analytical prospect it is essentially the same. Transferring data from point A to point B requires a lot of infrastructures to be in place in order to do so securely. This is why data handling is important in the IoT space.

Network

The last point of the literature analysis is the most important one as the network is the compilation of all the other topics discussed. This medium connects every other topic due to the nature of it being what is needed to actually physically transmit the binary bits from point A to B, no matter if they are encrypted, handled properly or accessed by a third party. Every author that has been read on the IoT security topic agrees that in one way or another networking is essential, due to the fact that the network connects all the devices.

As we learned in the theory IoT architecture is divided into three layers namely the Sensor Layer, Network Layer, and Application Layer. These once again indicate the network being in the middle of every aspect of IoT, and therefore possibly have the largest impact on the IoT space taking all the topics into consideration (Zhou, 2013).

In relation to the network being the transmission of the data to and from devices, the literature also showed that Wireless sensor networks are a dangerous environment due to its openness and often unattended way of being audited (Meghanathan, et al., 2010). In the regular theoretical aspect of Network security not based upon IoT we see that there are measures to take in order to segment the network into smaller pieces. This process is called subnetting and is a method to make the network infrastructure segmentation so that instead of one physical network you can divide it into multiple logical networks. This ultimately provides the network with multiple areas of conducting various job functions. One of the most common usages of this process is to create a subnet for administrative purposes, so that specific rights are required in order to access certain systems. (W. Stallings, 2012) For large scale networks it is required to obtain a certain level of documentation on each subnet in order to map out each subnet and here by being able to implement access control and other security measures, such as firewall zones between the subnets (Shinder, 2005).

Privacy

Privacy is the means of cryptography, which is why these more or less go hand in hand in the sense that one probably does not exist without the other. Privacy is the ability to have one's data stored securely so only the authorized users to the data can actually access it, the same goes for when the data is in transit. When you send an email you believe the email to be between the receiver and the sender, and you do not believe that anyone is eavesdropping on the network to potentially see your

clear text email. Due to the matter and the fact, we gathered in the cryptography paragraph, it is clear that IoT needs to ensure the user's privacy one way or the other. One of the key points mentioned in the literature surrounding privacy is that the user's privacy is threatened due to the limited control the individual user has over collected, distributed and redistributed data concerning them (Maras, 2015).

Furthermore it is mentioned in the theory that inference should at the minimum be very hard to conduct (Weber, 2010). This is classified by Weber as one of the challenges in relation to privacy in the IoT space. Inference is a data mining technique that can be performed by analyzing data in order to gain otherwise unobtainable information from a database (W. Stallings, 2012). This means that a user whether good or bad, from simple information gathering can put together more comprehensive data schemes which potentially can directly yield personal information being purposefully delivered by the data base even without the user directly asking for it. As a means to contain the situation it is proposed to establish Role-based systems and data governance where organizations see fit (Miorandi, et al., 2012).

Privacy for users is not only an IoT specific problem, but a more general problem which is why a few techniques for securing the user's privacy have been created, both techniques that I am going to mention is very commonly used in the world we live in today. This is why the literature also mentioned these two as being the primary tool towards securing user specific data from being interrupted during transit (W. Stallings, 2012; Weber, 2010).

The measures that can be taken in order to secure privacy standards are Virtual private network(VPN), Transport layer security (TLS), or even onion routing which is known from the TOR-network. In the IoT space for organizations onion routing might not be the ideal solution in almost any case, but we see VPNs and TLS being an integrated part of many larger firms this day in age (Weber, 2010).

Privacy is important in the security of IoT due to its nature of collecting data from various sources and since inference is a plausible security risk it can often be very complicated for the individual to know whether or not a third party for example can see when a specific person enters and leaves the office.

Cryptography

The means of cryptography is commonly referred to as encryption and decryption. What encryption set out to do is to mask humanly readable information into non-human readable information via a set of ciphers (Diffie & Hellman, 1976).

Data that flows from one device to another on a medium like a modern day network (can be both the internet and a local area network (LAN)) and can be subject to be tampered with or eavesdropped upon. (Diffie & Hellman, 1976) provide an example of a telephone line in their 1976 article that people are different and might have different wants and needs when it comes to security and cryptography. One person might find the telephone line secure enough to get his or hers message through to the receiving party. On the other hand a standardized telephone line might not be sufficient medium to get very sensitive data from point A to B, in the matter of transferring very personalized data. Recently in Denmark we have seen social security numbers in the hands of the wrong people due to errors on multiple sides of the data transfer (Mosskov, 2016). As the article states, due to the possibility of eavesdropping and other technological challenges the data is transferred to CD's, yet these were not encrypted which could have easily been done with the cryptography standards we have today. This shows that even though a technologically enhanced country as Denmark does not always apply the best practice methods. This prompts one to think that regular organizations most likely does not always perform best practices when it comes to transferring information over any type of media as the internet or any other digital medium.

As the example and the theory shows that cryptography is not always used even though it seems rather fortunate to use it, there has to be a reason for not implementing some sort of encryption to data transfers.

Encryption is divided into two type's namely symmetric encryption and asymmetric encryption. These have various functions that are similar but the distinction between the two is that the symmetric one use a shared-key to encrypt with, and the asymmetric method uses private and public keys. Ergo we have one key versus two keys.

As established the need for encryption when transferring data, especially private and business data this has to apply to IoT devices and systems as well. Regarding IoT and cryptography Uckelmann mentions the following, in a chapter on the challenges of developing IoT:

“Symmetric encryption algorithms seem not realistic, due to the necessary exchange of a common decryption key to all objects. However, the usage of the public key cryptography, which does not

require an exchange of a secret key, claims comprehensive computing time – potentially more than autonomous objects can offer or than their energy capacities can provide” (Uckelmann, 2011).

Due to many IoT devices being small lower powered devices it can be very hard to implement any type of encryption, or if it can be done the encryption methods used are often so low-practice that it is almost rendered useless in the sense that a 64 bit key is easier to guess than a 256 bit key.

Cryptography is hereby important for IoT setups due to no company purposefully and full aware would allow their data to flow over any type of network in clear text. The obstacle as we learned from Uckelmann is that at the time where he wrote the book architecting the internet of things, most devices barely had the capabilities to use cryptography at the scale that it is required, in order to do so securely in a business environment.

Access Control

Access control in the IoT space is limited in the sense that the access you actually can control stems from what setup there is on the network side of things. Besides that access control is a physical aspect from the literature as many authors categorize IoT devices as small unattended devices, with often unused ports such as USB and others (Atzori, et al., 2010). These ports can give unauthorized personal access to manipulate the devices. As soon as the devices are out of the companies sight it is a liability due to the fact that it has a connection to the network which makes most companies function properly this day in age (Meghanathan, et al., 2010).

This means that access control is divided into two categories, namely remote access control and physical access control. These two have the same purpose but are fulfilled very differently. Remote access control in the space of IoT devices is the ability for authorized users to be able to configure and control the devices from a remote location, via a subset of security measures such as secure shell (SSH) (Ylonen, 2006). This is a commonly used way of encrypting remote control of a system or device via shell commands. This method is widely used in the IT space and especially from a network perspective as all managed network devices (also many IoT devices) have the function of remote configuration, due to the nature of having multiple devices in various locations, this method has been in larger firms for a very long time.

With the ability to securely and remotely configure and control devices, with the right authorization it is necessary to address the other spectrum of access control, the physical aspect. The literature

states that physical access control is a necessary part of IoT in the case of IoT potentially being everywhere (Uckelmann, 2011). Physical access control can be a hard problem to tackle due to the devices having to be either wired or as in most cases have a wireless form for transmitting data back and forth which eliminates the possibility to encapsulate the devices in a box with a lock on it. In this case, we can look to how Wi-Fi has been implemented as the technology closest to what IoT is believed to be in an office environment. With the Wi-Fi access points we see many of these placed strategically in hard to reach places, yet they can still function.

Conclusive remarks

The six topics mentioned shows that there are a set of potential threats with introducing IoT devices into the organization. Most of the threats are an enlargement of threats that already lies within the context of having information systems, networks and data to transmit back and forth. As the literature states it is very important to be aware of the threats that potentially can be abused and being aware is the first step to take action towards a more secure environment. The essential threats that IoT bring with it into the organizations are the need for transparency and awareness of the full environment that the IoT is being implemented in first of all. Besides that, it requires an evaluation of the whole IoT system that is going to be implemented to see where the potential threats to the infrastructure might be.

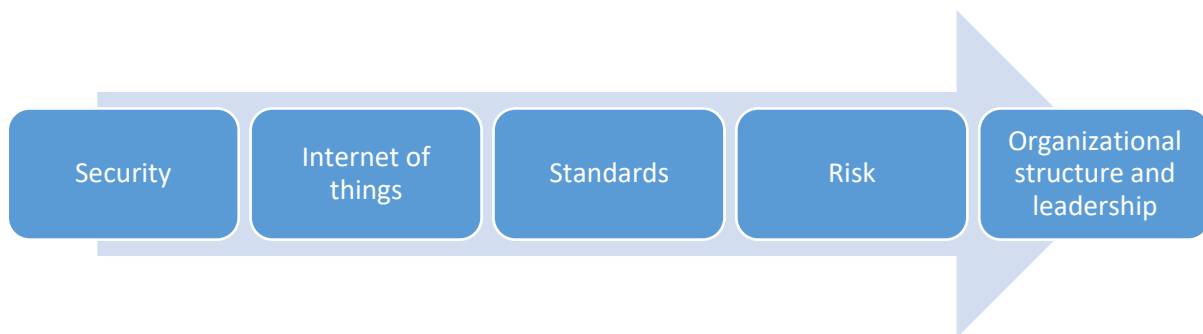
The clear obstacles are seen throughout the reading process and evaluation hereof is that they should see any device attached to the network infrastructure as a point of attack from anyone with malicious intents. This fact is accompanied by the need for establishing a way of encrypting the data to and from the devices in order to reduce potential privacy concerns.

Furthermore controlling access to the devices is also an essential point in the sense that due to the device now it is possible to control from outsiders even though they are not physically in the presence of the device. Alongside these threats it seems essential to thoroughly go through the network structure to see if the benefits outweigh the cost and to see if a new system is worth the risk.

5.3 Analytical model

Based on the observations in the literature findings I will create a statement for each of the topics in the conceptual framework in chapter 2.3. In order to see if these statements are true I will go

through the every topic in depth, and accompanied with answers from expert interviews to see if the statements are correct with the support of the empirical knowledge.



12 - Conceptualization

Security: IoT will increase existent- and provide new security-threats to information systems.

Internet of Things: Affects most employees and infrastructure one way or the other.

Risk: IoT requires that the organization conduct a risk analysis for involved systems before investing.

Standards: IoT does not fit perfectly directly into general security standards.

Organizational structure and leadership: Successful and secure implementation of IoT requires flexibility in organizational structure and dedicated leadership within the field.

To confirm or deny these statements there will be used the literature from the initial data gathering, which where to see what various aspects of security had an essential impact on IoT, as well as literature found in extension in the effort to dig deeper into the topics will be used.

5.3.1 Security

As the literature showed the most common security threats in regard to IoT is Cryptography, Privacy, Access Control, Data Handling and networking. These are therefore the baseline of what the following analysis on the topics deals with. The tendencies within these topics are that they are not IoT specific but rather normally found whenever security is mentioned. This confirms that the IoT technology is a collection of all other kinds of security, due to the large scale flexibility and interconnectivity with all other infrastructural systems that IoT affects one way or the other.

The literature shows that the cryptography needs more research in the sense that the lower powered devices cannot provide enough machine power to encrypt and decrypt data with a sufficient encryption method (Uckelmann, 2011).

The cryptography aspect is therefore an issue in many cases when it comes to IoT, obviously there are IoT solutions that have direct power connections to an outlet and are not run on battery but needless to say these devices are often appliances which are created by non-IT manufacturers which potentially can cause increased risk with bad developing or security measures hereof. (Lei Xu, 2016)

The literature on privacy states that it is important due to increased data gathering and potentially hereof more personal identifying data collected (Weber, 2010).

This means that organizations need to be aware that this is an issue for not only their business information but also their employee's sake. Identity theft increasing due to our more and more digitalized world and with IoT implementations this has a potential to increase further as there is gathered more and more data.

As more and more data is gathered it needs to be handled properly in the sense that it needs to be securely transmitted whenever it is being transferred from point A to B. Furthermore organizations need to be aware that whenever they store data there is a possibility that the data can be personally identifiable and therefore required to be stored securely. A common sentence in the world of IT is that: *"You cannot outsource responsibility"* (Chen, et al., 2015).

Access control is an important element for the devices that are connected to the various other services and systems that the company has (W. Stallings, 2012). The access control is deciding whether or not there is access to the device and is also the way that a company can control if it is the authorized users and/or devices that have access to the device. If the organizations did not calculate with access control the three parts of the CIA triad are potentially liable to be interrupted which causes the security and functionality of the system to be threatened (W. Stallings, 2012).

Access control requires maintenance so does the devices software and possibly the hardware in some scenarios. Maintenance of software is required as there are patches and updates to the devices operating systems or applications (Uckelmann, 2011). Besides the maintenance in some system installments there needs to be an audit of the output of the devices for the company to optimize the system performance or production.

The network in relation to IoT is obviously an essential part as there is no IoT without network connectivity. In most scenarios the networking infrastructure would most likely be sufficient to apply IoT but we naturally see increased operations in order to securely setup the environment to be capable to flawlessly implement IoT solutions with correctly configured access control, designated subnets etc. (Hermann, et al., u.d.). It is seen here that in relation to Networking it is most likely an enhancement of the requirements of the infrastructure depending on the imminent solution implementation.

The statement on security was that: IoT will enhance and provide new threats to information security.

As the section prescribes there will be a lot of enhancing as organizations introduce IoT into the companies. Furthermore it seems that there is a possibility for new threats in the sense that there are many new points of attack when you add new devices, and gather information from the sensors in the devices. The statement is hereby confirmed as there is both enhancing of already existent threats, but a very likely possibility of new threats emerging as the IoT technologies gain a more common status in the organizations.

5.3.2 Internet of Things

As the Flower model shows, Internet of Things is many things in compilation with each other and collectively they form the IoT space. Due to the multitude of IoT and all the aspects it brings together there are various parts the organizations need to be aware of before they venture into the IoT space. There might be some requirements from either their staff or their vendors in order to secure a healthy implementation and future operation of their solutions.

Introducing these systems and devices introduces new ways of attacking companies or using company facilities in malicious wrongdoings. We have seen refrigerators being a part of a botnet, (Xu & Perakovic, 2016) which allegedly can happen when security is not thought into the developing process when creating IoT enabled devices (Uckelmann, 2011). Having other devices than the normal PC enables the organizations to be eligible to new points of attack, due to all the various types of interfaces and sensors IoT brings with it.

Because there are new points of attack operational staff needs to know about the various software and hardware specific technicalities regarding the solutions (Uckelmann, 2011).

The operating system of the needs to be known by its operators in order to properly use the devices within the context it was meant to. The same goes for applications and how they work on the device. Some applications or systems might function differently or be faulty from the installment due to bad manufacturing and/or development (Atzori, et al., 2010).

It is not only the software that needs to be well rounded and exactly fitted to the specific system. The hardware side of things needs to be manufactured with high expertise as well, we learned in the structure and systems paragraph some manufacturers come from normally creating kitchen appliances and other non-IT related devices, and therefore they do not have expertise in how data security and hardware security should be manufactured to the same degree as for example large IT manufacturers like Cisco, HP, or the like that is known for quality IT products (Jing, et al., 2014).

The hardware and software side of IoT proves that employees are required to learn something about the devices if they are to handle them correctly. Furthermore IoT solutions might change processes for increased productivity which ultimately also has an impact on the employee's workflow.

The statement on IoT was that it affects the employees and infrastructure one way or the other. This is hereby also confirmed as we see both infrastructure and employees are potentially affected by IoT solutions.

5.3.3 Risks

Risk analysis should be part of any major decision, especially security decision which implementation of IoT systems inevitably is. The 6 step risk analysis by (Pfleeger, 2015) mentioned in chapter 2.2.4 is an excellent way of securing awareness of the potential risks that might occur. Risk assessments need to be conducted before acquiring any type of systems; in 2014 ISACA (previously known as Information Systems Audit and Control Association) created an infographic on IoT with multiple numbers on many of the topics covered in this report (ISACA, 2014). In the Risk section of the infographic it shows that in enterprises the Risk is 35 % versus Benefit in 31 % for IoT. For individuals the Risk is 30 % versus 46 % benefit. This shows that enterprises and organizations need to take into account that the Risk factor is higher, which can be explained by other aspects of the infographic. Under the Big Challenges section it is mentioned that security threats are increased by 49 %, data privacy by 25 % and below 10 % for identity and access management, compliance requirements, ownership of tech and/or data outside of it. 43 % of the respondents already have, or plan to have IoT strategy plans within 12 months (in 2015) (ISACA, 2014).

The statement for Risk was that IoT requires that the organization conduct a risk analysis for involved systems before investing. This is hereby confirmed with the survey-backed data from ISACA and the organizational knowhow alongside the appealing reasons provided by (Pfleeger, 2015).

5.3.4 Standards

As the delimitations states, the standard used in the report is the ISO27001, in addition to that I will introduce the PCDA model that is a four step model used to carry out changes. In the following paragraph, IoT specific knowledge on top of the standard in order to see where in the standard that IoT fits or where it might have faulty information about IoT will be provided. The ISO27001 Standard consists of 7 primary chapters, which includes both the thoughts previous and how to audit and improve the information security management system (ISMS) which the 27001 inevitably is, after it has been implemented. Due to the full cycle of 'Before, Under, After' that the standard has it is often combined with the PDCA as this provides continuous improvement and structure as time goes by and technology and threats change.

An evaluation and analysis of the ISO27001 standard will now show the important points in regard to IoT. The table below shows what point in ISO27001 is picked, with a reasoning behind how it has an effect on IoT.

Point	Description	Reasoning
4.2.A	Determine expectations	In any case, it is important to determine the expectations and goals for ISMS systems.
4.2.B	Interested parties requirements	Same as 4.2.A
5.1	Leadership with respect to ISMS	It is important that the leadership and management respects and complies with the rules set by the ISMS implementation. This is especially important in order to show leadership and having employees handle information with care to the ISMS system.
5.2	Secure the right policies	Much of the literature shows IoT as being technologically rooted, which ultimately gives the IT department a large quantity of work when getting IoT systems. Ergo the security policy needs to be appropriate in relation to the organization.
6.1.1	Address Risk and opportunities	As previously seen, there are both many risks and opportunities concerning IoT. It is therefore important to prevent undesired effects and focus

		on achieving a best possible outcome by creating proper plans.
6.1.2	IS Risk assessment	It is important to estimate and analyze the direct threats and plan for risk acceptance and evaluate the risk assessment process, by going through the documentation.
6.1.3	IS Risk treatment	In order to plan treatment processes correctly there should also be planned controls of mentioned processes. ISO27001 Annex A provides control objectives and controls.
7.1	Resources	It is essential to plan out the resource spending on not just implementing the system but also maintaining and to secure continual improvement
7.2	Competences	Organizations should evaluate if they have the right competencies to run the system based on the risk assessment.
7.3	Awareness	Any interaction with the system should be conducted within the parameters of the security policies.
8.1	Operations	Alongside 6.1 the organization needs to plan and control how to meet information security requirements.
9.1	Monitoring and analysis	The organization needs to evaluate the information security performance and effectiveness after implementation.
9.3	Review	A review should be conducted in order to ensure effectiveness and continuing suitability from the systems.
10.1	Improvement	As mentioned, it is essential so secure continuous improvement. The organization should conduct a plan for reacting to potential mishaps in relation to their risk assessment, and furthermore include how to take action to control and correct the mishaps and deal with the consequences.

As we see in the matrix, there is a lot of planning and continuity in the ISO27001 standard that also affects IoT. The essentials in the ISO27001 standard are that it is required by management to take action and responsibility for the systems they implement in regard to implementing an information security management system. Furthermore, it is built to secure proper planning, continuity and awareness in respect to information security. As the matrix also shows, there are gaps in comparison to the full ISO27001 standard, which is why only the points with relevance to IoT are selected. This selection is based upon the pointers gathered from the literature.

The PDCA model is applicable with the ISO27001 standard in every part of the model, as the following paragraph shows it can be combined with the findings in the ISO27001 standard as well as the literature on IoT and security in general.

Plan: To establish the ISMS policies, objectives procedures and relevant processes to managing risk and improve information security in accordance with the organization's security policies.

Do: Implementing and operating the ISMS policies, controls and processes.

Check: To monitor and review the process performance results against the policies, objectives and goals.

Act: Based on results take immediate and preventive action to achieve continual improvement of the systems.

By following these steps a continuity of any process is secured.

5.3.5 Organizational structure and leadership

IoT can potentially change the processes of the organizations as it can help in monitor production lines or accurately give real time information needed in other processes.

It is very individual how IoT systems affect an organization, department or process and that is why organizations should continuously identify if the systems are in line with the strategic goal and management wanted or if the strategy potentially should be considered a subject to change.

Due to the nature of processes being very dependent on the organization in question there is no common method of calculating improved productivity based on process improvement caused by IoT. (Jayavardhana Gubbi, 2013) It should be up to the single organization to secure measureable

numbers of improvement so it is possible to evaluate the investment and see whether the strategic goals are being met or not.

In order to leverage on IoT implementations we learned from the literature that having capacity in the organization is key. If there is no capacity on already existent infrastructure to apply IoT devices and systems the initial investment in hardware can be substantial.

IoT can hereby change the requirements put on the IT infrastructure in the organization, which needs to be addressed before investing in the technologies. If an IoT solution transfers more data than the infrastructure can handle on top of the data that is normally transmitted there might be bottlenecks and interference for the employee's normal work routines. When investing in IoT solutions this needs to be evaluated and can potentially exclude some manufacturers. When picking the manufacturer it is essential to secure that they have thought of system structure as well as security whilst developing the product. Today we see many non-IT manufacturers develop IoT devices even though they do not have the expertise and available competences to secure their products to a certain standard.

Furthermore the organizations investing in IoT solutions needs to be aware of increased workload for the IT department when they need to service and maintain these solutions.

The strategy includes having a plan for the future when it comes to IoT and overall 'on-going concern' thoughts. Having this mentality ensures that there has been a thought process behind every action taken when acquiring new technologies in order to increase either productivity or secure the growth of the business somehow.

As we learned from the Marshall & McKay model transformations requires strategy being thought into the process of transforming an organization. This establishes a long-term vision for the continued success of a company and in the IoT context, the leadership of the company needs to secure that there is a correlation between the IoT investments and how the organization sees itself in the long run. Otherwise, the investment might be an investment that adds zero value to the company in relation to its long-term goals.

Being on top with new technologies and trends that might help boost productivity or cut cost is essential in larger organizations to keep or a competitive advantage. It is important for an organization that wishes to leverage the IoT that they understand the long-term effects of the systems and can apply it in an already established strategic process. The CIA model and the IoT

section for architecture also show that strategy is an essential part of the effort of planning for the future of the company when it comes to choices on architectural and sustainable methods (W. Stallings, 2012; Uckelmann, 2011).

It is important to keep the strategic decisions continuously in order to always have both the long-term but also short-term goals in place and a plan to execute in order to achieve these goals. Especially in regard to IT as the industry changes so often and so fast, that there is a reason to believe that is so much of the literature suggests a close cooperation between IT management and business side of things (Austin, et al., u.d.). This is especially important when deciding the path the organization should take in relation to having the right competences to service equipment and secure that maintenance and operations, is done correctly but also by not overpaying for it.

5.4 Test of results

During the analytic review of the five topics in the conceptual framework I found out that the five statements mentioned in chapter 5.3 are in fact true. Whilst conducting the analysis I found that there are a lot of statements that needs to be verified or denied, and all of these originates out of the literature analysis. I will therefore verify or deny the statements that I came up with during the analysis of literature by comparing them to what the experts said about the concepts that were found in the literature. This makes the analysis complete as I have found out what the literature says, and tested that by combining it with the empirical data from the interviews.

The statements are indented and start with a dash as follows:

- There should be a precise purposeful strategy with the introduction of IoT.

The verification of this statement is dependent on the organization, as it was mentioned in interview 1 that the bike shop might not have the same requirements other larger organizations have (Interview 1, 2016). It is added that in other scenarios there will come a pressure from partners such as ISS that would want to add sensors and devices in towel racks, plants etc. so they can plan and optimize their work load (Interview 1, 2016). When the pressure comes from partnering firms to introduce IoT it is important to have a clear project plan so a number of potential pitfalls when it comes to security is as limited as possible. Experts agree with the statement.

- There should be organizational readiness for new technologies, as IoT procedures are not set in stone and IoT will introduce new complexities.

It is mentioned in interview 1 that the pressure from partners will be unavoidable in the long term as organizations will eat the potential cost saving that will be provided by partners as they can provide their services in the “smart office” cheaper with the introduction of IoT. This requires readiness for when the pressure comes and that every part of the organization involved can act accordingly when introducing the new technologies. It is also mentioned that the introduction of IoT devices is a branch of the ‘Bring Your Own Device’ phenomenon (Interview 1, 2016) and requires to be controlled by the IT department in order to securely implement it. This needs to be controlled by putting these devices out on their own subnet/vlan and a segment like that or maybe with new SSID structure so that there are SSID’s associated with different security levels and purposes. Experts agree with the statement.

- It is required to make sure who has the various responsibilities for the system and the infrastructure around it.

In interview 1, it is mentioned that there should be totally clear levels of how these devices should be. It is further mentioned that in the bike shop versus the large cooperation there is a large diversification between how such technologies is used (Interview 1, 2016). In interview 2, there is some consensus with the statements, as the respondent also says that there is a difference between small and larger corporations, but it is in general a good idea to secure that the properties of the device are up to par with the politics of the area (Interview 2, 2016).

In the ISS example in interview 1 it is mentioned that partners potentially can use their own networks SSID’s if wireless technologies are used, it can be added that in relation to network segmentation vlans for specific devices is a potential solution (Interview 1, 2016). Experts agree with the statement.

- There should be conducted a risk assessment, as new sensors and devices are connected to the network. This provides new points of attack, which is why a risk assessment is required.

“If you think from the perspective of a risk assessment you will be able to get answers to many of the questions, as in what are you trying to protect? What can threaten these values? What is important to accommodate these threats?” (Interview 2, 2016).

This shows that the method of creating a risk assessment is ideally a solution to grant awareness of various aspects of the security issues accompanied with an IoT solution. Based on the quote the experts also agree with this statement.

- Conduct an analysis of the communication interfaces attached to the devices in order to secure technologies used is aligned with security policies.

If you invest in IoT devices there will be specific demands depending on what device and its purpose are. An IoT Surveillance camera will have some requirements like strong access control, secure network protocols and encryption of data before transmitting it over the net (Interview 2, 2016; Interview 1, 2016).

In interview 1 it is mentioned that some due diligence is required on the desired devices and their capabilities before acquiring said devices. This fits on the communication interfaces, as this varies greatly from device to device, so based on the interviews this is also verified.

- Evaluate manufacturers of the devices, and potential partners. Evaluation should include how security measures are implemented into the devices.

As mentioned in the previous point, due diligence is important when you want to secure that the devices are properly made and have the right capabilities.

Furthermore in the ISS example mentioned in Interview 1, you need to secure that partnerships have the right standard of security so they comply with your standards so there is not all of a sudden a series of devices on your network with lower security clearance than you initially wanted to allow.

“There has been some cases with completely unsatisfactory security from large car manufacturers” (Interview 1, 2016). This shows that even larger corporations can have issues with creating devices that allow connectivity to the outside world. This quote in combination with the other data on due diligence points towards the statement is verified.

- Awareness regarding the physical placement of devices is essential, as physical access can be a security threat.

In regard to physical access control it is mentioned that Access Control in general this is a must in compilation with confidentiality and cryptographic measures (Interview 2, 2016). It is said that *“it depends on the company type ... in larger companies with a lot of traffic* (read: people and people

from the outside) *and the devices have more value physical access control is definitely a thing to keep an eye out for*" (Interview 2, 2016). Due to the generic nature of the guidelines this is hereby verified as it will apply to some cases.

- Secure that remote access to the devices is only for authorized users.

As the previous point stated, Access Control in general needs to be a thing in order to secure the devices. This is therefore also applicable to remote access control.

"The poorly manufactured devices have an embedded Linux on them and password is the root cause that was what was easy to remember" (Interview 1, 2016) if this is the case remote access control is very needed in order to secure such devices. Access control is hereby verified based on the nature of statements made in the interviews.

- Be aware of encryption capabilities of the devices so data transmission can be done securely.

In interview 1 it is mentioned that encryption is a large problem in IoT. It is mentioned that encryption requires good randomness in order to function well, and good randomness requires CPU power which ultimately costs money to put on the chips. *"IoT is created to be cheap, small chips with small power equals bad encryption, and you need good randomness in order to secure good encryption"* (Interview 1, 2016).

It is also said that *"Cryptography is important in special cases"* (Interview 2, 2016). Furthermore it is mentioned that there is a variance in the professional and private segment of the IoT devices. In the private segment it is mentioned that devices need to be cheap to sell them which allows manufacturers to skip on encryption methods, due to the cost of CPU power which is required. With that said, it is also said that in the professional segment this is where the serious vendors and manufacturers can stand out with a premium product even though it costs more (Interview 1, 2016).

The comparison is made between the professional segment and the private segment with an example of IoT cameras that should be encrypted when it streams data over the net, versus a coffee machine which not necessarily requires being encrypted as the data it sends is not critical in the

same way (Interview 1, 2016). Based on these findings it can be essential for some IoT devices to have encryption capabilities, and others might not need it. This does however verify the statement.

- Log actions were taken by the devices, and configurations made on the devices. This secures a way of surveilling the systems, and to go back and see what has happened in case it is needed.

Logging was mentioned in both interviews, however both respondents had agreed upon logging being a privilege that needed to happen on some sort of level, but it was not specific to IoT devices. Therefore further research is needed in order to validate this statement.

Due to the lack of information regarding logging is it hereby denied and discarded from the rest of the report.

- Be aware of any privacy issues and potential violations with the data collected by IoT devices and systems.

In interview 1 it is mentioned that there are some very clear rules in relation to privacy for example the cameras in the shops watching the register is one thing, but there should be a very clear indication of misconduct whenever a camera spotting an entrance is used to spy on an individual (Interview 1, 2016).

“If for example you have a cola vending machine and you bip your entry card every time you take one, then you risk that information is misused by showing that you might be going towards a bad health” (Interview 1, 2016). Privacy is therefore an issue which is why it is verified.

- Conduct a network analysis and segment the network so IoT only has access to what it needs access to in order to function. Some IoT systems might need access to production facilities while others just need an outlet to the internet. Subnetting and vlan management is a great tool for segmentation of the network.

In regard to vlans and subnets it is mentioned in interview 1 that it is important to reflect over how IoT devices are connected to the local network.

Furthermore it is added that you need to put IoT devices away into their own segment of the network so there is control with the liabilities and potential backdoors (Interview 1, 2016). This was mentioned as being a complete essential in any case when introducing potential liabilities into the network. It was mentioned that this correlates to BYOD as well, but here we have the possibility to put the devices “away” under their own segment on the network which was harder with the BYOD devices. This statement is verified due to the sheer evidence that both respondents mention network segmentation.

- Be sure to secure that there is interoperability between infrastructure and older systems and new IoT solutions.

When you introduce IoT you often introduce a potential backdoor in the organization's infrastructure. This ultimately makes information on the network and the network itself threatened. The respondent in interview 1 says that he saw that there was a DDOS network build upon IoT enabled cameras, this potential liability bears witness to the statement that if the network is poorly configured and barely secure, there is a potential risk with implementing these new devices onto it. And that is why there needs to be a collaboration between the administration of the infrastructure and the ones requiring IoT to be implemented. This statement is hereby verified by scenarios experienced in the real world.

Conclusive remarks

The statements from the literature conclusions are now tested with the expert knowledge from the interviews. As the chapter shows, most of the statements are confirmed, by either the same view or sentiment on the matter or a direct example, in which we can see that the statement is acknowledged in the context. However we do see that there is a gap in regard to logging; this was neither confirmed nor denied by the interviews. This shows that it needs further research in order to see if logging is an essential part of the IoT systems as we see it being with other systems (W. Stallings, 2012).

Furthermore we see that it varies from device to device what specific security threats that are in the spotlight. The empirical data indicates that there is a large gap between a random coffee machine with IoT capabilities and to larger enterprise surveillance systems. The differences between the two

are mainly the cryptographic aspect, but also how to segment the network in order to accommodate these new devices and purposefully use their strength and avoid the weaknesses.

The two most iconic tendencies brought forward in the interviews were that cryptography is hard and costly, but essential in some cases. Another tendency was that network infrastructure requires that you can put IoT devices out on its own subnet, so it is logically separated from other equipment attached to the network.

Chapter 6 Results

In the following chapter I will introduce the guidelines based upon the analysis of literature, expert knowledge and with input from the ISO27001 standard. Since most statements from the analysis were confirmed, many of these will appear in the guidelines, some of these are however too large and complex to be in just one point of the guidelines, which is why some are broken up into more specific smaller points of awareness.

See appendix 4 for deriving of ISO27001 context and the guidelines.

The guidelines are concatenated into three key areas which are 1 Strategy, 2 Organization, and 3 Network.

6.1 Guidelines

1. Strategy

The company should consider their strategical view on Internet of Things within the parameters listed below; these are the essentials points for creating an all-around strategy with all main topics to secure a strong generic IoT strategy.

1.1 Purpose

In order to decide how Internet of Things devices should be integrated into the company management should find out what their overall goal for these IoT devices is. This task should preferably be addressed with a series of representatives from multiple areas of the company. The representatives should be assisting the management in order to secure the goal is in alignment with the rest of the points under Strategy.

1.2 Financial costs

To run IoT devices has some costs attached to it, these should be identified. Some examples of costs to be considered are, operation, maintenance, initial costs of device and network equipment required for the device to be operational.

1.3 Risk:

Specific IoT device risks should be identified as Internet of Things security consists of multiple security areas. Some of those areas are: Internet security, Application security, Mobile security, Web security, Network security and system security. Due to the complexity of the security aspects, many of these are a potential risk, when acquiring IoT devices. The question management needs to ask is what potential attack surfaces the device has, in order to understand the risks involved.

Besides the various security aspects, there is potentially also risk attached to the employees working procedures and already established technical surroundings in the building in question. An assessment of the risk involved should be carried out by management before engaging in IoT activities.

In order to pick the right device for the strategical purpose and functions, some thought processes are required in order to achieve a best possible outcome, and avoid acquiring the wrong IoT devices.

1.4 Communication interfaces

In order to implement a secure set of IoT devices, the communication interfaces need to be identified. Having these identified before acquiring the device ensures that a device will be working in alignment with the overall goal from Point 1.1 – Furthermore it also ensures that the correct interfaces are present and that the device can communicate with the infrastructure it is supposed to work with.

1.5 Manufacturers

Before the devices are chosen, there should be conducted some form of due diligence on the manufacturers. Depending on how deeply the company wants to do this due diligence there are a set of questions worth investigating no matter what the situation is.

What is the manufacturers' core business? In terms of security there is a clear difference if the manufacturer's core business is to create kitchen appliances or they are a computer building company. Answering this question should give a good indication about the respectability of the

manufacturer when it comes to security. Furthermore it should also indicate whether security was involved in the design process of the product.

The next aspect of the manufacturers links to the first one, many of the companies that create IoT devices and solutions are not particular consistent when it comes to the architectural design of the software and how it well the device works in various environments. This means that often devices are not produced under a certain architectural specification and thereby it can be hard to integrate such devices with other it-infrastructure layouts than the one the manufacturer had in mind, when the device was created.

Some of the tendencies of products created without the consent of architectural standards some devices might have exposed USB ports, unnecessary communication interfaces such as Bluetooth, and even default passwords which cannot be changed.

Last but not least be aware of one-and-done companies, there are multiple eastern companies that create a few products and then close, which makes updates and maintenance a harder job in the future. Consider established firms as manufacturers.

1.6 Partners

Be aware of future potential requirements from partners such as cleaning companies, gardeners etc. these partners might pressure you into using your network to connect their IoT solutions in order to improve their workload. This is a potential risk.

2. Organization

The organization should consider their level of readiness to apply this new technology before investing in it.

2.1 Responsibility

Responsibilities for the various aspects of the devices need to be addressed, the most key responsibility is to address who is required in order to secure that the device is running properly. Examples of the responsibilities attached to a device could be to make sure that it is: functioning correctly, securely configured, and secured from unauthorized access.

2.2 Privacy

Depending on the IoT device, it might collect data that ultimately can be used to spy on employees in one way or another which is why Privacy is a key point to be aware of.

Make an assessment of whether the data collected by the IoT devices are in violation of employee privacy rights and if employees should be addressed with the new type of office environment in order to avoid problems regarding privacy.

2.3 Organizational readiness

Secure that you have the right competencies in the company to comply with the technologies that IoT introduce. Furthermore consider if any education of staff should be carried out.

2.4 Interoperability

Secure that there is interoperability among your existent equipment and security policies and the new IoT devices.

3. Network and security

- Be aware of encryption capabilities of the devices so data transmission can be done securely.
- Conduct a network analysis and segment the network so IoT only has access to what it needs access to in order to function. Some IoT systems might need access to production facilities while others just need an outlet to the internet. Subnetting and vlan management is a great tool for segmentation of the network.

3.1 Access Control

Access control is the measure to secure that devices are not accessible by unauthorized persons. Access control is divided into two categories, the physical access and the remote access both of which is equally important.

3.1.1 Physical access:

An assessment of physical access to the device should be conducted. This ensures that only purposeful interactions with the device are happening. Furthermore it also ensures that a common mistake is not made, since many fail to think about is that threats are not always external. Someone with physical access and bad intentions could potentially be an even larger threat than any external ones. Due to the potential internal threat, it could be valuable to secure the devices either by placing them strategically or in locked environments.

3.1.2 Remote Access:

Secure that only authorized personal have remote access to the devices. Remote access should only happen via specified channels in the security policies.

If the IoT devices need to interact with external sources like a partner or have other net-based interactions like the internet, extranet or intranet clear definitions of who and how remote access should be defined and maintained.

Other types of issues with remote access that should be dealt with are to avoid shared accounts, where possible only use the least privileges needed to fulfill the job and periodically review account privileges.

2.5 Encryption

Ensure that there are sufficient encryption capabilities on the devices if it is desired to not send data back and forth in clear text. Ask yourself if the data the device handles is business critical, or potentially privacy intruding.

3.3 Data handling

Data handling is an essential part of having IoT devices, since the main function of an IoT device is to obtain and transmit data, it is essential that devices are configured to send data to the right services and servers.

3.4 Sensitive data

Depending on the function of the IoT device, many of the devices are potentially carrying sensitive data in one way or another. All data that are collected and transferred through the device should be

assessed in order to secure that any business critical data or data that allows for direct person identification is transmitted securely. See point 3.2, 3.3.

3.5 Network segmentation

Make sure that if the network infrastructure allows it that it is segmented so that IoT devices can have their own space on the network, in order to limit the risk and lock-down the devices.

6.2 Discussion

The guidelines that sprung out of this report overall seem to be valid in the sense that other professionals in the field have yielded somewhat same results in the larger picture. The Danish company TDC (Hartig, 2016), Cisco (Cisco, 2015) and others such as FBI (FBI, 2015) mention many if not all the same areas as being important when working with IoT in an enterprise environment. By collecting this information and seeing that their results are very similar ensures me that the research conducted have yielded a positive result. On one side of things this ensures that the validity of the research, but on the other side of things I do feel that this research lack a number of interviews in order to diverse more into various examples and perhaps even decidedly cases in a real world environment. If I could have brought more interviews or a case company into the research the validity would without a doubt increase immensely. However there are limitations to the report, and one of the limits that hold the research back a little is the fact that there are only two interviews.

The research design chosen to create this research were a good method to secure that the right process was chosen. The inductive method by observing that the literature says in order to create a set of hypotheses which should be confirmed or denied secured that I read all the material and then testing the outcome hereof. Alternatively there would be potential for making assumptions of what statements should be tested, if the literature was not exhausted fully. So overall I feel the framework fits well, and it secured that the frame of the report did not steer out of the initial research question.

Chapter 7 Conclusive remarks

7.1 Conclusion

Internet of things is a concept which sprung from various connections between technological growth and evolution. The year 1999 is a big one in terms of IoT and its origin as Kevin Ashton coined the term "The Internet of Things". IoT has a large variety of possibilities, among others it is for example used for Industrial automation, smart homes, smart offices and smart cities. One of the most

appealing things about IoT is that it can be customized with a countless number of possibilities to provide automation and information, therefore also increase productivity and quality of work and the work environment in general. This is why there seem to be a pressure on companies to join the wave of IoT enabled solutions and as the research shows many of the companies have also identified how this technology development can benefit their operations in the future. Due to the development in IoT and the fact that companies now see a business strategy with IoT included is why there has been an increased focus and determination to gain the IoT advantages in the various organizations. However the IoT phenomenon does provide a series of challenges, both in terms of technological implementation but also in terms of security of their systems. Therefore the implementation and security awareness is a key point in order to obtain the goals set by the organizations.

Based on the description above there will be an answer to the following question, and sub-questions.

How can companies handle the introduction of IoT devices?

- **What essential security issues does IoT bring into the companies?**
- **How and to what degree should companies handle these security issues?**
- **Which security issues does ISO27001 Standard comply with, in conjunction to IoT?**

The goal with the report is to create and formulate a set of generic guidelines that can help organizations to securely implement IoT solutions by raising awareness of essential threats and pitfalls that apply to IoT. The guidelines should be generic due to the IoT phenomenon being so diverse that every company no matter what size or type can benefit from reading through it and hopefully avoid making any mistakes in their setup. The guidelines should serve as an answer to the overall question.

How can companies handle the introduction of IoT devices? – By following a set of guidelines that can raise awareness of the potential pitfalls and security threats that might be connected with the IoT solution.

In order to create the guidelines it is required to find the possible problems and issues surrounding IoT in multiple contexts. This was done by reading the literature on the subject and hereby finding out what the most common threats and problems were. As the commonalities of the threats and

problems arose, a list of statements was created, these statements were subject to get either verified or denied with data collected from interviews with experts in the IT security field.

The conclusion of the analysis is that most of the hypotheses can be verified however they are very dependent on the context in which the individual organization is in. The specific problem or threat to an IoT solution is also very dependent on the solution in itself as there are so many various types of solution benefitting and interacting with the organization in multiple ways.

Furthermore it was not only technological issues that arose. By implementing technologies like IoT there is allegedly so much influence in the rest of the organization that IoT can be mentioned to touch upon leadership and other organizational functions. The literature shows that it is very essential to plan ahead and create a strategy before introducing IoT solutions. By doing so the management can be on top of potential problems before they exist, many authors said IoT could be equated to an organizational transformation process which is why the McKay and Marshall Transformation process is included. This model provides a full generic method of handling transformations processes. By bringing in this model it was clear that some of the IoT related literature tried to apply some of the ideas behind the model, and furthermore with the association of the ISO27001 standard it is clear that any introduction of a new type of technology will have to undergo some of the effects that leadership and transformation processes have on an organization. In IoT this was no different based on the findings whilst going through the material. With IoT the transformation process was that it is required to think about what security threats IoT bring with it into the company network and secure that the organization is prepared to deal with it.

The essential security issues that IoT bring with it into the company are the various technological aspects of cryptography, access control, network security, privacy, and data handling. In most cases this is already potential security issues that the organizations have. However by introducing IoT solutions these issues will be enhanced and due to the nature of IoT it will also increase the points of attack.

In order to secure the organizations from these issues they should assess the amount of risks involved with their specific IoT solutions, and hereby within their means decide to what degree they should try to tackle these potential risks.

The ISO27001 standard proved to be useful for IoT in the generic sense. However there are areas in the standard where it is not so black and white while applying it on IoT. It was found that it is

important not to blindly follow a standard that is not specially tailored to a specific scenario as these standards are potentially not complete.

The sheer complexity of IoT can impact the organization in various ways, as the research shows it is therefore hard to create a comprehensive list with all issues and threats associated with the individual system. However the combination of standards and network related threats and solutions should make up for the most of the issues that can be with introducing IoT solutions.

Through the report it can be concluded that IoT potentially can have impact on various areas of the organization and therefore should be handled adequately with respect to risk assessments, organizational readiness and structure and last but definitely not least see how the IoT solution affects the context of which it is being implemented in with respect to network security. The last part is especially important as there can be a very large difference between small, medium and large organizations.

7.2 Reflection

The report sets out to create the generic set of guidelines that can introduce potential threats and problems by introducing IoT solutions into the companies. The initial idea for the report was to only base the report in the technological realm in term of security aspects. However while reading about the various topics that IoT contains, it quickly became clear that there is so much more to IoT implementations than just the security aspect, as a strategy for example. Furthermore it also quickly became clear that the most security threats were common with other systems and previous trends and therefore it seems that IoT does not provide so many new threats but rather enhances the existent ones. This yielded a few problems initially in regard to the overall goal and the research question, but due to the complexity of IoT and how it interacts and affects a large amount of the organization's infrastructure and personnel it became clear that this is also a threat and allowed for introductions to organizational theories. This gave depth in another way that was not anticipated from the beginning and it helped to secure the validity of the report.

In order to verify the hypotheses based on the literature two interviews were conducted, optimally I would have liked to have one or two more, maybe even with management level employees as they could give insight into the transformation processes and how they see it in their context. This would have given the data set more reliability and ultimately more depth to the report as these are only somewhat answered by the two existent interviews. In regard to the interviews it would also be a good idea if I were to re-do the studies, to conduct another interview with the same individuals and ask them about the set of guidelines directly. This would have given the guidelines more depth, and increase the validity of the guidelines.

As a method to verify and validate the findings and guidelines it would be ideal to test the guidelines in an implementation scenario in a few organizations. However this was not possible within the given timeframe as it proved to be very hard just to initialize contact and meetings with the experts.

Best case scenario would be to be able to test the guidelines on a case, to see whether or not they have an impact on the organization's way of thinking about how they should implement IoT.

7.3 Perspectivation

As the report shows internet of things has influence on many other topics as well. This means there can be drawn connections between IoT and many other things. During my studies I found that 'bring your own device' and 'Internet of everything' seem to be closely linked in two different ways however.

We have previously seen BYOD as a phenomenon that was unavoidable for the organizations, and to this day it is a very regular thing to encounter. I believe that IoT will be unavoidable in the same sense, that people will bring IoT enabled devices and ideas which will have to be utilized one way or another by the companies. And it might be viable for organizations to look back at the BYOD phenomenon and see the success stories and try to route their IoT endeavors towards that route.

Internet of everything (IoE) is another term that sprung in the studies as it is mentioned in the newer articles as a branch of IoT. IoE consists of two building blocks according to Cisco. These are: People, Things, Data and Processes, Cisco believe by combining these four blocks they can utilize IoE by establishing an end-to-end eco system of connected technologies, processes and concepts (Jaiswal, 2016)

References

- Allen, J. H., 2006. *CMU EDU*. [Online]
Available at: https://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_297130.pdf
[Accessed 28 7 2016].
- Alsaadi, E. & Tubaishat, A., 2015. Internet of Things: Features, Challenges, and Vulnerabilities. *International Journal of Advanced Computer Science and Information Technology (IJACSIT)*.
- Andersen, I., 2006. *Den Skinbarlige Virkelighed*. 3rd ed. Frederiksberg: samfundslitteratur.
- Ashton, K., 2009. That 'Internet of Things' Thing. *RFID Journal*, p. 1.
- Atzori, L., Iera, A. & Morabito, G., 2010. The Internet of Things: A survey. *Computer Networks*.
- Austin, R. D., Nolan, R. L. & O'Donn, S., n.d. *The adventure of an IT leader*. s.l.:HARVARD BUSINESS PRESS.
- Chen, F. et al., 2015. Data Mining for the Internet of Things: Literature Review and Challenges. *International Journal of Distributed Sensor Networks*, Volume 2015, p. 14.
- Cisco, 2015. *IoT Threat Environment*. San Jose: Cisco Whitepaper.
- Daya, B., 2013. Network Security: History, Importance, and Future.
- Diffie, W. & Hellman, M., 1976. *New directions in cryptography*, s.l.: s.n.
- Digst.dk, 2015. *Digst.dk*. [Online]
Available at: <http://www.digst.dk/Arkitektur-og-standarder/Videnscenter-for-implementering-af-ISO27001/Implementering-af-ISO27001/Hvad-er-ISO27001>
[Accessed 21 2 2016].
- EPOSS, I. &., 2008. *Internet of Things in 2020: Roadmap for the Future*. [Online]
Available at: http://www.smart-systems-integration.org/public/documents/publications/Internet-of-Things_in_2020_EC-EPoSS_Workshop_Report_2008_v3.pdf
[Accessed 1 3 2016].
- FBI, 2015. *IC3.gov*. [Online]
Available at: <https://www.ic3.gov/media/2015/150910.aspx>
[Accessed 4 11 2016].
- Forum, I. S., 2014. *Information Security Forum*. [Online]
Available at: https://www.securityforum.org/uploads/2015/02/Standard-of-Good-Practice-ES-2014_Marketing.pdf
[Accessed 13 3 2016].
- Gartner, 2015. *Gartner Hype Cycle*. [Online]
Available at: <http://www.gartner.com/newsroom/id/3114217>
[Accessed 1 March 2016].

- Giusto, D., Lera, A., Morabito, G. & Atzori, L., 2010. *The Internet of Things*. 2 ed. s.l.:Springer.
- Gubbi, J., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *ELSEVIER*, p. 16.
- Haller, S., 2009. *SAP: Internet of Things: An Integral Part of the Future Internet*. [Online]
Available at: http://services.future-internet.eu/images/1/16/A4_Things_Haller.pdf
[Accessed 13 2016].
- Haller, S., Karnouskos, S. & Christoph, S., 2010. *The Internet of Things in an Enterprise Context*, s.l.: Sensei-project.eu.
- Hartig, J. E., 2016. *Perspektiv.TDC*. [Online]
Available at: <http://perspektiv.tdc.dk/wp-content/uploads/kalins-pdf/singles/internet-of-things-8-noedvendige-sikkerhedstrin.pdf>
[Accessed 8 9 2016].
- Hermann, M., Pentek, T. & Otto, B., n.d. *Design Principles for Industrie 4.0 Scenarios*. s.l.:s.n.
- Hevner, A. R., Ram, S., Salvatore, M. T. & Jinsoo, P., 2004. Design Science in information systems research. *MISQ*.
- Interview 1, H. M., 2016. *Mærsk security officer*. [Sound Recording]. Appendix 1
- Interview 2, H. M., 2016. *IT Security teacher*. [Sound Recording]. Appendix 2
- ISACA, 2014. *IoT Infographic*. s.l.:ISACA.org.
- ISACA, 2016. *ISACA*. [Online]
Available at: <http://www.isaca.org/cobit/pages/default.aspx>
[Accessed 17 2 2016].
- ISO.org, 2013. *ISO.org*. [Online]
Available at: http://www.iso.org/iso/catalogue_detail?csnumber=54533
[Accessed 17 3 2016].
- Jaiswal, J. A., 2016. *IoT tech expo*. [Online]
Available at: <http://www.iottechexpo.com/2016/01/m2m/ioe-vs-iot-vs-m2m-whats-the-difference-and-does-it-matter/>
[Accessed 10 9 2016].
- Jayavardhana Gubbi, e. a., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *ELSEVIER*, p. 16.
- Jing, Q., Vasilakos, A. & Wan, J., 2014. *Security of the Internet of Things: perspectives and challenges*. New York: Springer Science+Business Media.

Kovatsch, M., Weiss, M. & Guinard, D., 2010. Embedding Internet Technology for Home Automation. *ETH Zurich*.

Kuhn, T. S., 1977. *The Essential Tension: Selected Studies in Scientific Tradition and Change*. Chicago: The University of Chicago Press.

Lei Xu, D. P., 2016. Cybersecurity and digital forensics. *International Journal of Cybersecurity and digital forensics*, 5(1).

Maras, M.-H., 2015. Internet of Things: security and privacy. *International Data Privacy Law*, 5(2).

Marshall, P. & McKay, J., 2004. *Strategic Management of E-Business*. s.l.:John Wiley.

Matthew Haughn, S. G., 2014. *TechTarget*. [Online]
Available at: <http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA>
[Accessed 2 6 2016].

Meghanathan, N., Boumerdassi, S., Chaki, N. & Nagamalai, D., 2010. *Recent Trends in Network Security and Applications*. s.l.:Springer.

Miorandi, D., Sicari, S., Pellegrini, F. D. & Chlamtac, I., 2012. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*.

Moore, G. E., 1965. Cramming more components onto integrated circuits. *Electronics*, 38(8), p. 6.

Moskov, M., 2016. *TV2*. [Online]
Available at: <http://nyheder.tv2.dk/samfund/2016-07-20-cpr-fadaese-nyt-lavpunkt-i-amatoeragtig-datahaandtering>
[Accessed 21 7 2016].

Pfleeger, C. P., 2015. *Security in Computing*. 5 ed. s.l.:Prentice Hall.

Qiu, T., Ding, Y., Xia, F. & Ma, H., 2012. A Search Strategy of Level-Based Flooding for the Internet of Things. *MDPI.com*, 12.

Ronald Moen, C. N., n.d. *pkpinc.com*. [Online]
Available at: <http://pkpinc.com/files/NA01MoenNormanFullpaper.pdf>
[Accessed 7 8 2016].

Rouse, M., 2015. *Internetofthingsagenda Techtarget*. [Online]
Available at: <http://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security>
[Accessed 16 4 2016].

Rowland, C., 2015. *Designing Connected Products*. 1 ed. s.l.:O Reily.

S. Deering, R. H., 1998. *ietf.org*. [Online]
Available at: <https://tools.ietf.org/pdf/rfc2460.pdf>
[Accessed 6 3 2016].

Shinder, D., 2005. *TechRepublic*. [Online]
Available at: <http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/>
[Accessed 5 2016].

Stallings, W. & Brown, . L., 2012. *Computer Security, Principles and Practice*. s.l.:s.n.

Uckelmann, D., 2011. *Architecting the Internet of Things*. s.l.:Springer.

W. Stallings, L. B., 2012. *Computer Security, Principles and Practice*. s.l.:s.n.

Weber, R. H., 2010. Internet of Things – New security and privacy challenges. *Computer Law & Security Report*.

Webster, J. & Watson, R. T., 2002. Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 6.

Xu, L. & Perakovic, D., 2016. Cybersecurity and digital forensics. *International Journal of Cybersecurity and digital forensics*, 5(1).

Ylonen, T., 2006. *IETF org*. [Online]
Available at: <https://tools.ietf.org/html/rfc4251>
[Accessed 13 5 2016].

Zhou, H., 2013. *The Internet Of Things In The Cloud..* s.l.:Boca Raton: CRC Press, Taylor & Francis Group, 2013. Print..

Figures and tables

- 1 – Google trend : Page 5
- 2 – CIA Model : Page 10
- 3 – Daya 2013 : Page 12
- 4 – IoT Flowermodel : Page 13
- 5 – IoT Transfer Mediums : Page 13
- 6 - PDCA Model : Page 16
- 7 – McKay & Marshall model : Page 19
- 8 - Conceptualization : Page 21
- 9 : Inductive : Page 28
- 10 – Design science : Page 28
- 11 – Concept Matrix : Page 31
- 12 – Conceptualization : Page 45
- 13 – Correlation ISO27001 & IoT : Page 49,50

Appendices

Appendix 1 - ISO 27000 Series

ISO/IEC 27000 — Information security management systems — Overview and vocabulary

ISO/IEC 27001 — Information technology - Security Techniques - Information security management systems

ISO/IEC 27002 — Code of practice for information security management

ISO/IEC 27003 — Information security management system implementation guidance

ISO/IEC 27004 — Information security management — Measurement

ISO/IEC 27005 — Information security risk management

ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27007 — Guidelines for information security management systems auditing (focused on the management system)

ISO/IEC TR 27008 — Guidance for auditors on ISMS controls (focused on the information security controls)

ISO/IEC 27010 — Information security management for inter-sector and inter-organizational communications

ISO/IEC 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

ISO/IEC 27013 — Guideline on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

ISO/IEC 27014 — Information security governance.

ISO/IEC TR 27015 — Information security management guidelines for financial services

ISO/IEC 27017 — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018 — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27031 — Guidelines for information and communication technology readiness for business continuity

ISO/IEC 27032 — Guideline for cybersecurity

ISO/IEC 27033-1 — Network security - Part 1: Overview and concepts

ISO/IEC 27033-2 — Network security - Part 2: Guidelines for the design and implementation of network security

ISO/IEC 27033-3 — Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues

ISO/IEC 27033-5 — Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

ISO/IEC 27034-1 — Application security - Part 1: Guideline for application security

ISO/IEC 27035 — Information security incident management

ISO/IEC 27036-3 — Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security

ISO/IEC 27037 — Guidelines for identification, collection, acquisition and preservation of digital evidence

ISO 27799 — Information security management in health using ISO/IEC 27002. The purpose of ISO 27799 is to provide guidance to health organizations and other holders of personal health information on how to protect such information via implementation of ISO/IEC 27002.

Appendix 2 – Literature matrix (reading guide)

The following picture is a snippet of what the whole sheet looks like. This however gives a great idea to how the reading has progressed. After each article has been read, notes were taken and added by the next column, in order to secure no knowledge would be lost in the process.

#	Author	Title
1	A Search Strategy of Level-Based Flooding for the	Tie Qiu, Yanhong Ding, Feng Xia * and Hongli
2	Architecting the internet of things	Dieter Uckelmann, et al.
3	Computer Security, Principles and Practice	William Stallings, Lawrie Brown
4	Enabling Things to Talk	Alessandro Bassi, et al.
5	Future Internet	John, Domingue, Dieter Fensel
6	Internet of Things: security and privacyimplication	Marie-Helen Maras
7	Internet of Things – New security and privacy chal	Rolf H. Weber
8	Internet of Things: Features, Challenges, and Vuln	Ebraheim Alsaadi, Abdallah Tubaishat
9	Internet of Things (IoT): A vision, architectural ele	Jayavardhana Gubbi, et al.
10	Recent Trends in Network Security and Applicatio	Natarajan Meghanathan, et al.
11	Risk-Based Adaptive Security for Smart IoT in eHe	Habtamu Abie, Ilanko Balasingham
12	Security of the Internet of Things: perspectives an	Qi Jing • Athanasios V. Vasilakos • Jiafu Wan
13	The Internet of Things	Daniel Giusto, et al.
14	Designing Connected Products	Claire Rowland, et al.
15	DESIGN SCIENCE IN INFORMATION, SYSTEMS RESEAR	Alan R. Hevner, et al.
16	Abusing the Internet of Things	Nitesh Dhanjani
17	Embedding Internet Technology for Home Automa	Matthias Kovatsch, Markus Weiss, Dominique
18	The Internet of Things: A survey	Luigi Atzori a, Antonio Iera b, Giacomo Morab
19	The Internet of Things in the Cloud	Honbo Zhou
20	Designing the Internet of Things	Adrian McEwen, Hakim Cassimally
21	Smart Community: An Internet of Things Applicatio	Xu Li, et al.
22	A systematic review of RFID	Kwangho Jung and Sabinne Lee
23	Proposed Security Model and Threat Taxonomy for	Sachin Babar*, Parikshit Mahalle, Antonietta
24	Security Architecture on the Trusting internet of th	Bing Zhang, Xin-Xin Ma, and Zhi-Guang Qin
25	Network Security: History, Importance, and Future	Bhavya Daya
26	Data Mining for the Internet of Things: Literature I	Feng Chen, Pan Deng, Jiafu Wan, Daqiang Zha
27	Internet of things: Vision, applications and resea	Daniele Miorandi, Sabrina Sicari, Francesco D
28	Cybersecurity and digital forensics	Lei Xu, Dragan Perakovic
29	what we have yet to learn about software risk management	
30	IPV6	S. Deering, R. Hinden
31	Security in Computing	Charles P. Pfleeger, Shari Lawrence Pfleeger, J
32	Internet of Things security and privacy: Design me	Yacine Challal, et al. 2015
33	Information SecurityTheory and Practice	David Naccache Damien Sauveron
34	Insecurity in the Internet of Things	Mario Ballano Barcena, Candid Wueest
35	Interoperability of Security-Enabled Internet of Th	Sarfraz Alam, Mohammad M. R. Chowdhury, Jo
36	STRATEGIC PRINCIPLES FOR SECURING THE INTERNE	U.S. Department of Homeland Security
37	The CEO's Guide to Securing the Internet of Things	AT&T Cybersecurity Insights Volume 2
38	The Identity Of Things: Privacy and Security Concer	Simon Moffatt MBCS, CISSP
39	Internet of Things Architecture	Alexandru Serbanati, et al.
40	The Internet of Things in an Enterprise Context	Stephan Haller, Stamatis Karnouskos, Christo
41	IoT threat environment	Cisco Whitepaper

Appendix 3 – Interview guide

- Introduction
 - IoT devices
 - Verify what the literature has said about IoT security
 - Etc.
- Job description
- Security:
- Access control
 - Physical Access control
 - Remote Access control
- Control with data handling
- Privacy
 - Sensitive data
 - Should employees know about data collection
- Data transmission
 - Cryptography
 - Encryption
 - Decryption
 - Protocols
- Logging
 - Data logs, changes etc.
- Network:
 - Vlan & subnet
 - DMZ zones
 - Firewall
- Organizational perspective:
 - Manufacturer choices
 - Software vs hardware requirements
 - Manufacturers core business (Appliances vs security)
- Are IoT devices in alignment with the security policies and strategies?
 - Classify data

Appendix 4 - ISO versus IoT Map

Guideline number	ISO27001 Correlation	ISO27001 Control measures
1.1	4.2A 4.2B	A.14.1 A.14.2
1.2		
1.3	6.1 10.1	A.11.2.1
1.4	5.2	
1.5	5.2	A.15 A.11.2
1.6	4.3	A.15
2.1	5.1	A.12.1
2.2	5.1	A.18.1.4
2.3	4.2	A.5.1 A.6.1
2.4	9.3	A.5.1 A.6.1
3.1	9.1	A.13.1
3.2	10.1	A.13.2 A.18.1.5
3.3	7.1 7.2 7.3	A.13.2
3.4	7.1 7.2 7.3	A.13.2
3.5	7.1 7.2 7.3	A.13.1.3 A.12.1

Appendix 5 – Interview 1

Hvad er din stilling?

Security manager, Mærsk

En af de store områder inden for IoT er ifølge litteraturen Access Control, både fysisk og remote, er det noget du generelt kan genkende?

Nu udtaler du internet of shit forkert.

Ja der er lidt der i form af sikkerheden

Ja – Jeg tror det er det i form af access control der er de fleste iot devices på wireless ehh og langt de fleste professionelle accesspoints har mulighed for flere SSID's som rent faktisk gør du har flere forskellige virtuelle accesspoints og der er det det er fornuftig at have et separat ssid til dine iot devices, sådan at de kommer ud af access pointet på et separat vlan, som er et virtuelt kablet netværk. Og så ryger det ind i en helt separat del af dit netværk så den dag der er noget galt på dine devices og passwordet til det her ssid bliver kendt, og alternativt at du ikke kan skifte det her ssid password fordi så skal du rundt og skifte det på 300 devices der sidder alle mulige mærkelige steder, i køleskabe osv der skal flyttes ud fra væggen og have indsat specielle koder osv.

De fleste har en klar politik at et password skifter du hver 3 måned f.eks alt efter hvordan sikkerheden er og med iot devices er du nødt til at lave en eller anden form for mitigation af den risiko du har ved at have dem på dit netværk, og det gør du så .. synes jeg i hvert fald ved at smide dem ud på et separat ssid og sige okay det er så et throwaway ssid, hvis det bliver overtaget er det selvfølgelig ikke godt men det er jo stadigvæk bedre end hvis det netværk som resten af vores pc'er og servere osv kører på.

Så det du siger er at både at remote mæssigt der vil det være en løsning at køre vlan og separerer fuldstændigt ved hjælp af firewall og styre det den vej igennem?

Ja

Hvad med fysisk foreksempel? – er der et eller andet formål med at kameraer sidder 3 meter højt for eksempel så de ikke er lige til at tilgå eller er der noget der skal låses inde?

Altså kameraer .. hvis du sætter kamera op er det fordi du ønsker den data strøm der kommer ud skal være tilgængelig for folk der har adgang til den ikke.

Ja

Hvis vi er dybt naive og antager at det er sikkert det der er lavet og det kan kun læses af dem der skal, så har du selvfølgelig sat kameraet der hvor det giver mening og derhen hvor det skal bruges og ikke andre steder hen, det er den naive verden ikke.

Der er generelt to metoder du kan lave det her på med internet devices som jeg har oplevet ikke. Du har hvad skal vi sige, nye og moderne som sidder på nettet og skyder data til en server, så kan du

hente det fra den server der. Det virker fint for hjemmebrugere, hvor det bare kobler på via dhcp, og så skal du ikke kende noget til dit netværk og alle er glade ikke.

Det tror jeg ikke du får nogen til at gøre i en virksomhed tror jeg, så skal du ned i cykelhandler osv, og det er sikkert fint for dem også fordi de har et helt andet trussels billede. Hvorimod sådan en virksomhed som her ikke, der vil det helt klart være sådan jamen vi kan godt sætte nogen wireless kamera op, ind på ssid og så fyre det ned til vores centrale video optagning, men for det første vil det være sådan at nu er det wireless og afhængig det er hvor fortroligt de data der kører henover den wireless forbindelse de er så vil det være okay at gøre der over wireless eller ikke okay at gøre det over wireless – hvis vi antager indgangen i receptionen her, så er der selvfølgelig fortroligt hvem vi har kommende af gæster her, men det kan du også sætte dig ned med tele linse, eller på en plastik stol og holde øje med selv så det er jo ikke hemmeligt vel. Så det vil jo selvfølgelig være okay at sende over iot , altså ikke ud på internettet i første omgang med så det ender på vores servere, det var der engang noget der hed action kamera der gjorde for 15 år siden dengang jeg begyndte på det her..

Hvis du har et kamera der øhh holder øje med direktørens pengeskab vil det helt klart fange hans pin-kode og så er det ikke okay det køre over wireless, og det er måske ikke engang okay det bliver optaget på et bånd.

I det eksempel vil du sige, at vi kan ikke have et kamera der fordi det som det optager er voldsomt fortroligt, og det kan ikke køre over nettet. – Det skal kables op – Så der vil være nogen hvor ej det kan vi ikke have på wireless.

Så det du siger er i det store hele der er meget forskel på hvilket device og sammenhængen?

Du er nødt til at se på det som den bliver brugt til, de data der kommer ud af det- hvilken form for klassifikation har de data og så har du en sikkerheds politik der siger hvordan du behandler de data ud fra kvalifikationen, og når du så har de to ting koblet op på hinanden indlysende hvordan du skal gøre det.

Så pengeskabet for direktøren må så ikke gå over public net, og på trådløs osv. – Derimod cykelhandleren der har de nok kamera primært imod tyve, og tyve vil ikke sætte sig ned og hacke leverandøren i kina som har den her hub stående og tage vores kamera feed og planlægge et indbrud. Fordi det gør tyve der rammer en cykelhandel generelt ikke vel. Så der vil det være okay for dem, men for os vil det være helt uacceptabelt ikke.

Så der er helt klart niveauer for hvordan de her devices skal være ikke, det device du sætter på kaffemaskinen for at holde øje med om den løber tør for bønner – ja okay worst case er så vi løber tør kaffe på den her etage ved at jamme den her sender ikke. Ja okay det overlever man nok. Firmaet går ikke ned på det i hvert fald.

Nu nævner du selv data håndtering, hvilket også er det næste punkt og privacy for de ansatte skal virksomheder fortælle deres ansatte hvilke data der bliver indsamlet?

Ja du har nogen helt klare regler i .. jeg tror det er .. der er en eller anden lov om ansættelse og kameraer. Og hvis kameraer kan se præcis hvad du laver må du generelt ikke gøre det, der skal være en god grund til det.

F.eks de kameraer der sidder nede i brugsen og kigger over kassen netop for at kunne se hvad der sker om der bliver snydt, der er et hjørne af reglerne de bruger der ikke, hvorimod de kamera der ser folk gå ind af en bygning skal ikke være tilgængelig til alle.

Det skal ikke være sådan at chefen skal kunne sætte sig ned og se xyz kom igen 10 minutter forsent i dag den holder ikke.

Samtidig med der også er regler for adgangskort, den log skal være lukket ned så kun hvis der er mistanke om misbrug i området, eller de mener jeg er en fupper der kommer efter arbejds tid og løber med kuglepennene – så der er klare regler som man skal forholde sig til, det betyder også at hvis du f.eks har en cola automat hvor du bipper hver gang du tager en cola så kan du risikere det kommer ind på de her personfølsomme data, om at xyz drikker godt nok mange cola med sukker i, måske han er på vej ud i et misbrug – eller den er måske ikke så slem, men der er regler omkring de her følsomme data.

For at data skal være personfølsomme skal de være koblet til et individ og givet at du kan lave store gæt på hvem individet er i mange tilfælde, så er det jo ikke en tæt kobling direkte.

Hvis nu vi var en ambassade eller lignende, så ville du have en anden situation og så kan det godt være du ville sige at alt hvad der overhovedet kan indikere om der er folk i bygningen kan klassificeres som kritisk og så må du igen .. så har du igen de data du har og dem klassificere du efter din sikkerhedspolitik og så igen køber det sammen og se lige præcis her er det ikke okay at man f.eks via potteplanterne kan gætte på hvor varmt der er i lokalet for at se om der er nogen og så skal det evt køres meget stramt, ellers skal du slet ikke gøre det.

Du nævnte data transmission, i den forstand kan du så nævnte et eksempel hvor man kunne sige her et det super kritisk at alle sikkerheds kriterier så som kryptografi og protokoller og et andet eksempel hvor du måske bare ville sende ud på nettet som du har lyst til?

Hvis vi forlader den corporate verden, og du har et kamera der tager billeder af dit barn – babymonitor, så kan du sidde og se om dit barn har det godt osv, den datastrøm går så over til en server i kina, og så videre til din telefon – Hvad kunne problemet være? Jo problemet er at hvis nogen opsnapper den her datastrøm og bruger det som børneporno, er ungen kommet til skade? Nok ikke, og det er heller ikke relevant for diskussionen for hvis folk føler sig krænket, så føler de sig krænket ikke. Derfor er det vigtigt at som du selv siger der er en krypterings protokol som gør dataen er overført hensigtsmæssigt krypteret, så er det specielt data adressed hos leverandøren i kina er det meget vigtigere, for der er det de er lette at angribe, fordi det er der det hele går sammen ikke. Så de er nødt til at gemme det som krypteret data, men sker det? det tror jeg ikke fordi kryptering er svært og det koster cpu kræft.

Ja det koster penge i den lange ende

Ja såå eh det bør være krypteret ja. Det modsatte eksempel er kaffemaskinen som siger kom og tøm mig, men igen du kan måske skabe lidt trængsel nede hos baristaen nede på hjørnet ikke, men derudover er det jo ikke det store problem og så bliver folk nødt til at drikke en kop vand i stedet for kaffe.

Dertil sagt eh så de IoT ting skal jo laves fordi det skal være billigt, så små chips med små hjerner dermed dårlig kryptering. Kryptering er super afhængig af du har noget god randomness, og i de devices er der ikke god randomness i generelt.

IoT devices har ikke så meget cpu kræft så det med at implementere en stærk krypterings algoritme er måske ikke lige det som der er plads til når de nu skal komprimere dataen fra kameraet, sende det over nettet osv., så der vil du have et problem med at gøre det her sikkert nok. Hvis du undersøger det er der sikkert massere af kameraer der har det her problem.

Det er en af de helt store aspekter i det med kameraer, det er jo netop at de skipper de steder så det kan gøre billigere ikk.

Jeg tror også du har oplevet af der er to klasser af iot enheder, der er dem der er rettet imod consumer og dem der er rettet imod corporate. Der var nogen der lavede en aftale om levering af 25.000 iot devices for ISS. Dem vil jeg tro bruger et helt andet niveau af iot devices .. jeg gætter, men de vil skulle sikre sig at de har en længere levetid en den almindelige forbruger.

Igen jeg gætter, du har to typer devices – det professionelle og de dumme brugere, og det professionelle vil du selvfølgelig kunne sige okay den er prof, så den kommer med lidt mere markup og plads til lidt mere cpu og lidt mere randomness så du rent faktisk får en forbindelse så du kan gøre de her ting.

Igen det kræver du tænker over det, og det er der sgu mange der ikke gør.

Det er lige det segment hvor min opgave gerne skulle dukke op, med at der er nogen af de her punkter man skal være opmærksomme på når man investere i de her ting. Ligesom da folk begyndte at tage deres computer med, i bring your own device som var det tidligere store, det kommer jo også til at ske med IOT devices tænker jeg. Det bringer os videre til at snakke om loggning.

Skal vi logge kun på virksomhedens ting ..

Generelt skal du logge ting der kører i dit netværk – at der har været den her og den her forbindelse så man kan se hvad fanden skete der her ikke? Og der vil det være ret fedt at have indholdet men igen som vi snakkede om tidligere med overvågning af brugere og ansatte, hvis de kvajer sig og deres mails bliver hentet i klar tekst så står det hele pludselig i loggen, også den mail de fik fra deres læge. Og så er vi ude i dybt personlige oplysninger hvor der er strænge krav til opbevaring fra datatilsynet så det er der mange der vil sige det tør vi ikke.

Det er for og imod, til hverdag er det mere lettere at håndtere dataene, men når du har et incident ville det være rart at have al information.

Der er ikke one size fits all her, din sikkerhedspolitik skal være gennemtænkt, også for iot devices. Og der vil det nok være at de fleste sikkerhedspolitikker skal køres igennem engang til i forhold til iot devices, for det har man ikke tænkt over dengang de er blevet lavet.

IoT er jo ikke andet end et par år gammelt så det er vigtigt at der bliver ændret i politikkerne.

Ja den seneste ISO 27001 er fra 2013, så den er 3 år gammel – så der er nok lidt man kunne tage med..

Ja

Du nævner selv netværk og vlan osv, men i forhold til virksomheds perspektivet og valg af producenter der nok er professionelt og noget til consumer, men i forhold til producenter er der nogen forhold hvor du tænker hvordan vi skal håndtere de her ting og sager?

Igen. Sikkerheds politikken siger at du skal skifte password hver x dage, og det er fuldstændigt urealistisk at rende rundt til alle planterne og skifte password på dem, så der har du selvfølgelig nogen exceptions fra de regler. Du ved så du har de her regler men jeg ved også det er umuligt at skifte password på plante monitorne, så de kører default. Remote på de her devices er nok mest throw away, og har nok noget nul-setup config, hvor den spørger efter dhcp for at komme på.

De dårligt produceret devices har nok en embedded linux på den, og password der er root for det var det man lige kunne huske ikke.

Ja så kan du benytte den til hvad du har lyst til ikke.

Ja, ehm og der vil du jo igen på mere professionelt niveau nok have en lokal hub du smider data til så de ikke ryger til kina, ehh igen som vi snakkede om tidligere om du holder data på nettet eller lader det komme ud.

Mit eksempel var hvidevare og biler, de har nok ikke den store it sikkerhed inkorporeret i deres..

Ja biler, de har jo haft fuldstændig været utilfredsstillende sikret selv fra store leverandører. Der var et eksempel hvor to hackere efter aftale hackede en journalists bil, hvor han måtte bede dem stoppe fordi han blev utryk. Der var masse ballade om det i to timer, og så var folk videre fordi det tænker vi ikke så meget over, der kommer en masse omkring det her – allerede i dag har du jo dæktrykmåler i dækkende som du kan spoofe hvis du er tilstrækkelig ond, i starten var de helt uden autentikering så du kunne køre op på siden af en bil og sige jeg har pludselig 0 dæktryk og så siger bilen selvfølgelig ahh 0 dæktryk og begynder at bremse ned ikke. Jeg tror de har lavet noget paring med værksted osv nu så man ikke så let kan gøre det udefra nu. Men igen de der små skod enheder – hvor meget processing kan du forvente af dem? Hvis du skyder 5 millioner pakker af, kan du så gætte den rigtige og komme igennem?

Måske ja

Ja

Ja, så du siger når du skal vælge producent fremover så er der formål med at vælge en producent der har tidligere erfaring?

Du skal lave din due diligence når du vælger producent, og overfor din producent vil du skulle sige: Argumenter overfor mig for, at din sikkerhed på det her er i orden, og hvad har du gjort – hvilke antagelser har du gjort? Det ville jo være dumt at købe noget der var sikret imod alt hvis du er en virksomhed som os, fordi det ville være at smide penge ud af vinduet.

Virksomheden skal redegøre for at deres sikkerhed er i orden og deres software udvikling er fornuftig. Selvfølgelig kan de lyve, og så igen er vi ude i at du har et stort PR hit hvis det sker ikke. Så vælg en virksomhed som ikke er "fire and run" med deres produkter som mange taiwan producenter er, de laver et produkt og et halvt år efter er de væk.

Inden for den sidste uges tid var der nogen der opdagede et ddos netværk der var bygget på adskillige tusinde kameraer som var i pressen her.

Det er ikke lang tid siden jeg også læste om et hvor køleskabe var inkluderet i forskellige botnets.

Ja. Det sker jo nu

Det sidste spørgsmål her det er sådan set hvordan IoT og politikkerne skal passe sammen? Vi har jo den her nye trend hvor det er næsten umuligt at vi skal have de her ting ind over.

Vi har jo ISS til at varetage rengøring og faciliteter her ikke, og det vil fra dem blive et krav at de skal sætte en lille måler ind i håndklæde automaten på toiletterne så den selv kan sige nu er den løbet tør for håndklæder. Det pres vil komme den anden vej ikke. Det samme med planter så de ved hvornår de skal vandes.

Virksomhederne vil æde det her op fordi nu kan de måske have en mand hver anden dag i stedet for hver dag, fordi opgaverne bliver optimeret. Så ja der vil være et pres der er fuldstændigt umuligt for virksomhederne at undgå det på sigt ja.

Det var faktisk det, du har rundet mange gode eksempler som kan bruges i

Appendix 6 – Interview 2

Hvad er din stilling?

Underviser i IT.

En af de store områder inden for IoT er ifølge litteraturen Access Control, både fysisk og remote, er det noget du generelt kan genkende?

Ja, både og. Altså access control er jo en generel ting som benyttes i sikkerhedsøjemed inden for IT, så af den grund er det også helt klart en vigtig ting at holde øje med når vi kobler diverse IoT devices på netværket.

Er der forskel på vigtigheden alt efter om det er remote eller fysisk?

Det kommer an på løsningen og virksomheden vil jeg sige.

Ehh altså remote er jo altid vigtig når vi snakker netværk, fordi man oftest har remote adgang til sådanne enheder. Fysisk er vel mere i takt med om noget skal låses inde.

Hvis du nu har et kamera der sidder 3 meter højt for eksempel, så det altså ikke er let at tilgå er det så okay, eller skal sådan noget låses inde?

Lige kamera sætter man oftest så de ikke kræver yderligere for at udføre deres funktion, derimod er der meget andet udstyr som netværks udstyr der gerne er låst inde af forskellige årsager men det er igen alt efter hvilken virksomhed du er. Der hjemme låser man heller ikke sin router fast fordi man får gæster man ikke kender så godt. Så i mindre virksomheder hvilket man kan relatere til at benytte de her devices derhjemme, så tror jeg ikke det er relevant. Men i større virksomheder hvor der er meget trafik, og udstyret derefter også har større værdi det er fysisk access control helt sikkert en del der er værd at holde øje med.

I forhold til data handling og privacy for de ansatte skal virksomhederne så fortælle om hvad der bliver indsamlet til deres ansatte?

Ja det vil jeg helt klart mene. Ehm der skabes så meget data nu – altså der skabes så meget data som kan bruges til det ene og det andet hvis man kører dem sammen teknologisk.

Altså sammenhængen mellem forskellige data kilder kan udnyttes hvis man får adgang til dem?

Ja præcis. Hehe altså det er jo langt fra alt data som er under privacy banneret, og det er da også kun noget special data som f.eks persondataloven retter sig imod, men med de her devices vil der være

øget opmærksomhed på den type data også, så det er helt klart et vigtigt punkt når vi snakker iot devices i visse sammenhænge. Måske som kameraer osv, det er nok ikke så vigtigt hvis støvsugeren er iot.

Når du nu nævner kameraer, så er det jo en form for data der kan bryde privacy reglerne. I den sammenhæng skal der så være specielle protokoller og kryptering inden over i et virksomheds miljø?

Helt klart, jo mere kryptering jo bedre. Det er bare svært på de her små devices. Mange iot devices er jo sådan noget småt noget som bare sender få signaler ud fra deres sensorer. Dette gør de ikke har kraft til at lave god kryptering.

Hvad med specifikke protokoller?

Jeg mener ikke der er nogen protokoller som er specifikt bedre til at sikre iot end almindelig data transfers. Igen vil jeg fremhæve at de her devices er uden den store kræft så ofte er det faktisk ikke muligt at påføre andet end en meget simple type kryptering. Ehh altså det jeg mener er at siden der ikke er power nok i dem så kan de jo ikke lave god kryptering da det ville tage alt for langt tid for enheden, og derved kan de ikke skabe den værdi som de er indkøbt til.

Okay, så du mener ikke kryptering er så vigtigt fordi diverse devices ikke kan håndtere det fornuftigt?

Altså jo kryptering er vigtigt – men i specielle sammenhænge, hvis vi tager iot kamera så er det vigtigt vi ikke kan opsnappe det feed som kameraet sender, hvis det sendes i ukrypteret form. Derimod er der sikkert mange andre små devices hvor det ville være en umulighed og også mere eller mindre ligemeget.

Hvis vi tænker i en virksomheds sammenhæng, måske mellemstor, og stor virksomhed?

Jo større virksomheden er jo større er kravene vel også for at der er styr på hvordan dataene flyder rundt på deres netværk.

Skal denne data logges?

Altså dataen på netværket?

Ehm ja, altså data der kommer fra diverse iot devices rundt omkring, måske fra pottedplanter, kameraer osv.

Logging er altid en god ting.. ehm igen tror jeg det kommer meget an på virksomheden og på det device de har anskaffet sig. Såfremt der er mulighed for at logge aktivitet så skal det helst gøres så man kan finde ud af hvad der er gået galt hvis nået går ned.

I forhold til netværk så hørte jeg i et andet interview jeg har lavet at iot devices der benytter wireless skal sendes ud på deres eget ssid og vlan, hvad synes du om den ide?

Det er helt klart fremgangsmåden. Hvis vi taler virksomheder som har en vis størrelse så er vlans og den type segmentering en naturlig ting at gøre.

Man får en helt klar opdeling af netværket hvis man gør det på den måde, og så klarer netværket selv at sende data frem og tilbage i de forskellige virtuelle netværk.

Så det vil være med til at øge sikkerheden ved iot devices at de kommer på deres eget net?

Helt sikkert. Så kan man sætte sig til at lytte på iot nettet hvis man har sådan et for at finde ud af om der er ting der sker, som ikke skal ske. Så er alle iot devices også virtuelt gemt væk fra andre dele af nettet så som virksomhedens servere.

Ja det er rigtigt – hvis vi går videre til den organisatoriske del og snakker om forholdet til valg af producenter er der så noget du tænker man skal være specielt opmærksom på?

Hmm ... alt efter hvad der købes så er det jo forskelligt. Men igen den store virksomhed vil nok skulle screene deres leverandører mere end en frisør skulle.

Ja, for at være sikker på at få opdateringer, og lukket sikkerhedsmæssige huller?

Ja det er altid en god ide at have en vis form for service når man køber IT udstyr, jeg tror dog kun at sådan noget som service level agreements SLA's som du sikkert kender.. ehh er noget som bruges ved større virksomheder som køber store løsninger inden for iot.

Det er altså en god ide at vælge en producent der har erfaring med opdateringer osv?

Ja en IT mæssig leverandør burde jo have styr på sådan noget.

Ja selvfølgelig .. okay det sidste spørgsmål er faktisk hvordan IoT og politikker skal passe sammen? Altså det jeg mener er at det er umuligt at undgå IOT nok bliver en del af virksomhedens netværk på den ene måde eller anden, så hvordan skal disse stemme overens?

Hvis jeg forstår dig ret så skal politikker jo altid være opdateret, så hvis vi får nye devices ind så skal politikken opdateres derefter. Er det svar ok?

Tjæ, hvis jeg nu nævner at man kan have en politik som siger man skal benytte ISO27001 hvordan skal iot så passes ind der?

Så vidt jeg husker er IoT ikke en specifik del af den standard du nævner. Ehm hmm iot er dog ikke så specifik, som jeg sagde tidligere så er det en god ide med netværks omdeling, altså de her segmenteret vlans som vi snakkede om. Det er jo ikke kun godt til iot men også til alt andet som servere og pcer og printere. Derudover hvis du tænker på et risiko perspektivet ind her vil du være i stand til at få svar på mange af de spørgsmål man kan stille i den sammenhæng. Ehm altså hvad er det du prøvet at beskytte? Og hvad truer disse ting? Så kan du finde ud af hvad der er vigtigt for at undgå eller forsøge at undgå disse trusler.

..

Men altså sikkerheds politikken skal være opdateret, så den passer på den type udstyr man benytter.

Ja det lyder meget fornuftigt, det kan jeg godt genkende fra andre interviews og fra mine undersøgelser jeg tror faktisk det var det sidste spørgsmål, så jeg vil sige tak.

Selvtak.