LUND UNIVERSITY

School of Economics and Management

Department of Informatics

Cyber Security in Smart Cities

Not a primary concern

Master thesis 15 HEC, course INFM10 in Information Systems

Authors: Gustav Jansäter
Joel Olsson

Supervisor: Odd Steen

Examiners: Bo Andersson
Miranda Kajtazi

Cyber Security in Smart Cities: Not a primary concern

AUTHORS: Gustav Jansäter and Joel Olsson

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

PRESENTED: June, 2018

DOCUMENT TYPE: Master Thesis

NUMBER OF PAGES: 108

KEY WORDS: smart city, cyber security, information security, IoT, smart initiatives

ABSTRACT (MAX. 200 WORDS):
Smart city is a phenomenon here to stay and constantly evolving and expanding and is fast becoming a paradigm for the transformation of connected cities. More and more parts of cities are being connected and with it, the risks and issues are on the rise. However, smart city projects often overlook the pervasive cyber security risks and threats that permeates these initiatives. The endeavour of this research paper is to explore and identify the various factors affecting the lack of focus on cyber security in smart cities. The study found multiple factors that had implications upon the amount of focus on cyber security. The study outlines an intricate web of factors for lacking cyber security in smart cities that have multidirectional effect upon each other. The paper also acknowledges that there is an intrinsic issue in regards to what level of cyber security is sufficient, but suggests that the current focus on cyber security is reactive rather than proactive, which creates innate and critical problems for the future.

Content

Figures

Tables

1 Introduction

Smart cities is a highly contemporary phenomenon with vast amounts of resources and time being spent on developing various application areas with connected technology. The main aim of these projects is to increase quality of life for inhabitants in urban areas and comes as a response to the many different problems that comes with densely populated urban areas. Smart city as a phenomenon being practiced has for three decades been developed and practiced (Pierce, Ricciardi and Zardini, 2017). The smart city projects vary in their application areas, ranging from connected waste bins to ‘smart’ building automation appliances.

Even though the term ‘smart city’ is being widely noted and used, it is a surprising challenge to exactly define the boundaries of this concept, something, which many agrees upon (Hollands, 2008; Nam and Pardo, 2011; Zanella et al. 2014;). Despite this, Curry et al. (2016) defines the concept of smart cities as a “Complex Socio-technical system of systems” which will be aptly named as a *constellation of systems* further on in this paper. Yadav et al. (2017) describe smart city as a concept where difficult city issues are tackled by integrating information and communication technologies (ICT) with the urban city infrastructure in order to create a equitable and sustainable system.

There are several broad spectra initiatives from high instances such as from the European Union called the European Initiative on Smart Cities but also smaller initiatives such as EU-gugle and Smart City Sweden. The main focus of these initiatives is to create smart and sustainable city solutions.

The potential for an increased well being with smart city initiatives is great (Chakravorti and Chaturvedi, 2017) and can be applied to different areas, as previously mentioned. Examples range from more effective traffic flows, more efficient waste management, less energy consumption - especially in both housing and offices, which is seen as an incredible decrease in energy consumption as buildings in general constitutes two thirds of general energy consumption (Dell and Intel, 2016). Zanella et al. (2014) offers the explanation that smart cities aim to improve and be a part of a wide range of new services offered to citizens, companies as well as public administrations. They argue that automation in both homes and industries, as well as medical aids and elderly assistance, intelligent energy management and smart grids will be affected and more effective.

Many believe that the ‘smart society’ that we are moving toward is similar to the ones featured in sci-fi movies and other culture mediums, which is something Chakravorti and Chaturvedi (2017) describes as while being farfetched to some degree, it is no less vivid. They instead conclude that the smart city projects are subtler in its’ way of affecting our everyday lives in various useful and present ways. Chakravorti and Chaturvedi (2017) claim that there are three main results of smart city projects, namely; the overall wellbeing of citizens of urban areas, increased efficiency of institutions as well as a more powerful economy.

Zanella et al. (2014) assert that smart cities are founded on information communication technology (ICT) as well as Internet of things (IoT) devices. They mention that the IoT devices, everyday objects filled with *“micro-controllers, transceivers for digital communication, and suitable protocol stacks….”* have had a revolutionary impact and is a paradigm for the future. The goal, they mention, is to achieve are more immersive and pervasive Internet. They do, however, conclude that there is a lack of standardised policies and best-practice because of its “novelty and complexity” which is something that has to be overcome for the bright future of smart cities to be realised.

1.1 Cyber Security

According to The International Telecommunications Unions (Telecommunication Standardization Sector of ITU, 2008), cyber security is defined as:

> *”Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.”(ITU-T, 2008, p. 2)*

Elmaghraby and Losavio (2014) defines cyber security in the aspect of cyber security as such; *“Security includes illegal access to information and attacks causing physical disruptions in service availability.”*

Cyber security is often analogous to the term information security and used together to describe the security of an organisation’s information infrastructure. Von Solms and van Niekerk (2013) argue that while the two concepts are heavily similar, they are not, however, exactly the same. Instead, they mention, cyber security encompasses yet another dimension of security, namely the one of defending human lives from cyber attacks, which is something that is highly current considering the pervasiveness of information systems in critical infrastructure, especially in smart city urban areas where incidents may affect human lives adversely.

Our interpretations of the two separate terms are very similar considering the nature of this paper’s research area. By protecting the information systems in smart city applications (information security) human lives are, likewise, safer (the added aspect of cyber security) considering the physical actuation of these systems in the real world. We are, then, expanding the term of information security in the application of smart city contexts which then becomes analogous to cyber security due to the latter’s goal of protecting human lives.

1.2 Problem Area

The smart city initiatives are often associated with an increase of connectedness, by way of connected devices often named “Internet of Things” (Kyriazis et al., 2013; Petrolo, Loscri and Mitton, 2014). Internet of things (IoT) devices are described by Jin et al. (2013) as excellent data gathering tools and communicating this data to a central location for further use. IoT are often found as sensors or actuators - where they can command and control simple things in the “real world” from a digital command.

As with almost all new technologies, however, there are of course drawbacks. The main one, many would argue, is the fact that a more connected society and everyday life leaves more openings on being attacked digitally in an emerging new crime category called ‘cybercrime’ (Yar, 2006). One thing attributed to IoT is the lack of security and EY (2016) mentions in a report the lack of hardware security as an insecure feature in smart city societies. Potoczny-Jones (2015) also argues for the insecure ways of IoT, arguing that IoT went for “the lowest-hanging fruit of security” that is passwords which has led to massive attacks using the hacked devices as slaves performing a distributed denial of service attacks (DDoS) like Mirai and a very recently discovered new huge botnet (Check Point Research, 2017).

Cyber security incidents seem to be be occurring with increased frequency (Yar, 2006) and there are multiple examples pertaining smart cities. A rather recent example of this is an incident in 2011 where a water pump was destroyed due to a cyber attack on a city water station in the town of Springfield, Illinois (Zetter, 2011). Another example also happened in the U.S. which targeted Dallas, Texas (Rosenberg and Salam, 2017) and the attackers assumed control of the warning sirens of the city and proceeded to activate them for several hours during the night. Another, more life-threatening example was found by an employee of Kaspersky Labs, Denis Legezo (2016). During an investigation on the security of connected traffic lights, he succeeded in his attempt of hacking and accessing the traffic lights in central Moscow which gave him complete control of said traffic lights.

An example of IoT and the risk of contamination from unsecure devices for the greater whole occurred earlier this year (Williams-Grut, 2018) in which hackers succeed in infecting and hacking a fish tank thermometer in the lobby and from it managed to access the casino’s high-rollers database and export it.

Pierce and Andersson (2017) highlight several different challenges for smart cities to overcome and list information security as one of these, as well as one of the three most occurring challenges in regards to the technical challenges domain. They mention that smart cities will need to have urban systems that achieves and upholds a high-level interoperability because of the fusions of ICT and IoT. Due to the high complexity and interdependency of these systems, Al-Dairi and Tawalbeh (2017) argues that there is a greater attack area for malicious actors. John-Green and Watson (2014) mention that there is a certain hyperconnectivity of IoT devices and urban systems and acknowledge that this entails various problems, which they categorise in four different characteristics, namely hyperconnectivity, loss of boundary, complexity and industrialised hacking.

Cyber security needs to be a primary focus in smart cities in order to counteract building buggy and brittle cities (Townsend, 2013; Kitchin, 2014). Furthermore, Townsend (2013) state that it is not a matter *if* the digital foundation of smart cities will fail, it is *when* and how much damage it will cause. With that in mind, previous cyber-attacks that target the city infrastructure have already caused damage. For instance, in Israel hacktivists managed to cause a traffic congestion for eight hours (Paganini, 2013). Khatoun and Zeadally (2016) conclude that with the threat of cyber attacks, cyber security needs to be addressed in a proactive manner when implementing smart city projects.

Yet with everything that has been established above, cyber security is often not considered as a challenge, which is something Pierce and Andersson (2017) and Wenge et al. (2014) conclude. Furthermore, information security or cyber security is not a challenge that is mentioned, alternatively previously recognised but rather as a non-challenge for smart city initiatives by practitioners and decision makers (Bakıcı, Almirall and Wareham, 2013; Pierce and Andersson, 2017). After an extensive literature review, no studies have been found that indicate that cyber security in a smart city is a challenge, actively treated or untreated, recognised by decision takers.

This research paper will explore the focus or attention on cyber security actions that have been taken in smart city projects. By focus, this paper denotes the amount of attention or consideration given to an issue and also the amount of attention the solution is given. Previous literature has presented that the issue with cyber security is a non-challenge (Pierce and Andersson, 2017) and that it is not usually a primary concern nor a focus in smart city projects. We are interested in finding out why. We are limiting ourselves to ‘cyber security’ issues, and disregard the possible ethical concerns of privacy in smart cities.

1.3 Research Question

What are the reasons for the lack of focus on cyber security in smart city projects?

This research question is based on prior research ascertaining that cyber security is not a primary concern for smart city projects which has been established in the previous paragraphs.

1.4 Purpose

What is concluded is that cyber security is important as the consequences from breaches range from mortal danger to large economical losses. The literature rarely looks into the combination of smart city phenomena and cyber security and has failed to reach a conclusive paradigm regarding these two concepts which is why we want to explore why there is a certain lack of focus on cyber security in smart city projects according to previous literature.

In order to achieve this purpose, the study follows a qualitative approach by way of semi-structured interviews. As an outline for the interviews, a theoretical model based on previous literature will be used. The model will identify factors and categorize these in common, overarching themes for a clearer structure. The interviews will follow a script formed with the model as a basis. The interviews will then serve as the data collection and be analysed with the help of coding formed from the common themes identified earlier. Thereafter, a discussion will be formed about the experiences from the respondents and compared with previous literature.

The endeavoured contribution to the IS field of study is to explore the reason why there is a lack of focus on cyber security within the smart city context, especially when security is a pressing issue in most other IS fields.

1.5 Delimitation

The study will be limited to cyber security, which is defined as:
”Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.” (ITU-T, 2008 cited by von Solms and van Niekerk, 2013).

This study will only focus on cyber security and will not discuss the ethical issues with privacy involved with cyber security.

2 Smart city and cyber security

When conducting our extensive literature review we found that the lack of a proper and unified definition of the concept smart city and its components which became the first objective (see 2.1). Next, this paper explores the cyber security of the IoT devices (see 2.2), which are widely used and crucial to smart cities (Elmaghraby and Losavio, 2014).

In smart city initiatives project leaders do not perceive cyber security as a challenge (Washburn and Sindhu, 2010; Wenge et al. 2014; Pierce and Andersson, 2017) and since no research has explored the reasons behind the lack of focus specifically in smart city projects, this study resulted in a framework of different possible factors that lead to the project leaders lack of focus (see 2.4 for the descriptions of the factors and 2.5 for the framework).

2.1 Smart city

The concept of smart cities lacks a common definition (Hollands, 2008; Negre, Rosenthal-Sabroux, Gascó, 2017), which leads to a variety of smart city definitions. Yadav et al. (2017) describe smart cities as a concept that handles difficult city issues with the help of advanced ICT (information and communication technologies) and the urban infrastructure, citizens and city managers in order to create an equal and sustainable city. Furthermore, Curry et al. (2016) describe smart cities as a "Complex Socio-technical System of Systems". Baccarne, Mechant and Schuurman (2014) describe smart cities as a city of the future with digital technologies enabling cities to become more green, accessible and liveable. This study's perception of smart cities argues that as stated by Harrison et al. (2010) that smart cities involve the cities which connect physical, social, business and IT infrastructure in order to leverage the intelligence of the city as a whole. Furthermore, the overall goal is to improve the quality of life and operational efficiency with the help of emerging technology (Harrison et al., 2010). Thus, the three components for powering smart city initiatives are physical infrastructure, social infrastructure and technology.

The next section will describe these three components in further detail in order to clarify the meaning of each component. *The physical infrastructure* can, for instance, include roads, bridges, water, power and airports (Hall et al., 2000). *The social infrastructure* consists of resources that assist education, health care, intellectual capital and social capital (Nam and Pardo, 2011). Lastly and most important in smart cities is the component of *technology*. Prominent municipalities have taken advantage of technology in order to create efficient services for their citizens by utilizing sensors, data storage devices, computers and extensive analysis (Jin et al. 2013). The authors describe IoT (Internet of Things) as a core pillar in smart cities, which enables the possibility to create a urban information framework which provides interoperability between services in the city. The wireless and broadband network as well as service-oriented information systems etc. is vital for leveraging the collective intelligence in smart cities (Chourabi et al., 2012).

However, as mentioned by Pierce and Andersson (2017) technology does not achieve the sole purpose of smart cities on its own. Rather, technology is a mean to support integration between the other elements involved in order to achieve stated goals. Nam and Pardo (2011) argues that smart city initiatives require urban planning based on governance with involved stakeholders and institutional preparations in order to be successful. Furthermore, global sustainability is expected to embrace an international and over-border approach in order to connect companies and territories for success (Attour et al., 2015). Mauser et al. (2013) similarly describe that global sustainability is created in interaction between civil society, governments and other stakeholders and does not emerge soly from science. Thus, this paper argues that smart city initiatives is leverage through collaboration between cities in line with what Pierce and Andersson (2017), Mauser et al. (2013) and Attour et al. (2015) describe.

2.1.1 Smart city actors

Although the components of smart cities are rather clear, the actors, which are involved, are not always as evident. Yadav et al. (2017) describes citizens as crucial actors in the smart city context. Moreover, Dameri and Rosenthal-Sabroux (2014) also argue that in order to enable smart cities, citizens play a vital role for the social and technical transformation needed for this. That is to say, the citizens are both producers and consumers of the generated information in smart cities (Dameri and Rosenthal-Sabroux, 2014). Furthermore, smart cities aims at increasing citizens' life quality and thus, a smart city requires a comprehensive security of the highest level to ensure the stability of this quality of life (Bartoli et al., 2011). Leydesdorff and Deakin (2011) describe three other actors by applying the triple-helix model - shown in figure 2.1.1.1 below - to cities. The authors outline that interactions between universities, industries and their government generate an constantly changing premise for cities. In other words the general goal of smart cities outlined by Harrison et al. (2010) describe the three components for powering a smart city initiative; physical infrastructure, social infrastructure and technology. The four actors that collaborate with the identified components in order to tackle the challenges of growing urbanization are; the government, industries, universities and the civil society.

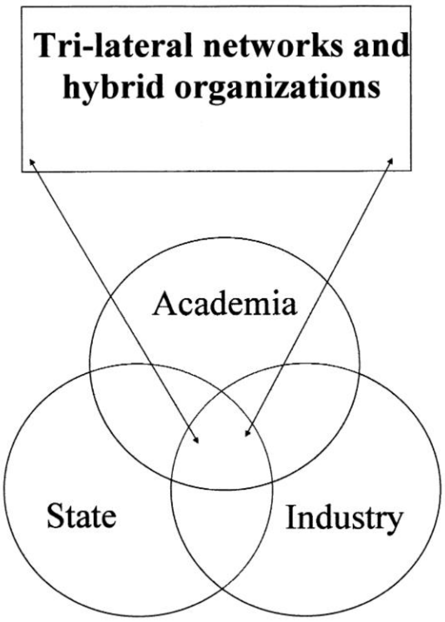

Figure 2.1.1.1: The Triple Helix Model of University–Industry–Government Relations. (Etzkowitz and Leydesdorff, 2000, p. 111)

The next section will describe the actors shown in previous figure 2.1.1.1; universities, governments and industries, in further detail in order to clarify the meaning of each actor. Firstly, *universities* are not only a platform for education, it can also work as a platform for networking which results in connecting entrepreneurs, companies and scholars in order to create innovative solutions for urban problems at hand (Kraus et al., 2015).

The government controls the platform upon which the smart city projects are built and also connects stakeholders as well as determine the interaction between the other actors (Dameri and Rosenthal-Sabroux, 2014). Furthermore, both transnational and national governments have provided funding and support for smart city initiatives (Baccarne, Merchant and Schuurman, 2014). The governmental support of smart city projects boosts the initiatives worldwide (Baccarne, Mechant and Schuurman, 2014) and thus, both the national and transnational government have a key role in decisions and strategies of smart cities. With that said, municipalities also play a key role in concerning smart city support, decisions and strategies but require support from EU-programs as well as industries due to financial limitations (Dameri and Rosenthal-Sabroux, 2014).

Cooke and De Propris (2011) describe that *industries* have a central role in creating regional and national value as well as innovation. The industries have pressure to innovate in order to stay competitive which results in innovation spiral (Baccarne, Mechant and Schuurman, 2014). Thus, the emerging technology from industries is required to further develop and enable new technical solutions in smart cities.

In conclusion, smart cities are influenced by the collaboration between the three components; *physical infrastructure, social infrastructure* and *technology* and the four actors; *government, industries, universities* and *the civil society*. Smart cities are also influenced by the collaboration between smart cities, and it is in the constellations of smart cities that development and innovation thrive.

2.2 Smart city and IoT

Elmaghraby and Losavio (2014) claim that IoT and smart cities are tightly knit together and Baig et al. (2017) argues that IoT is an enabling technological innovation combined with cloud platforms. The way these devices communicate is by way of machine-to-machine communication. Klinpratum et al. (2014) assert that M2M communication is essential for the existence of IoT. Cha et al. (2009) note that machine-to-machine (M2M) communication is the eventual paradigm in wireless communication and that there is currently a monumental increase of machine-to-machine equipment (M2ME) which will continue to increase in the forthcoming years. Pötsch et al. (2013) agrees and explains that M2M communication technology is mainly machines communicating to with each other without the intervention of humans. They argue that M2M communication will be pervasive in various application fields and areas. They mention that research and standardisation has yet to reach formal conclusions when it comes to the structure of M2M communication and the equipment using it.

2.2.1 Cyber security and IoT

Jin et al. (2014) proposes a framework for IoT integration with complete urban ICT systems and note there are several problems to overcome before unlocking a complete smart city area. One of these problems is the unsecure features of IoT devices for a large scale applicable use as, in an industry report by EY (2016) note the lack of standardisation and overall insecurity of these devices which then leads to the greater risk of potential antagonists to feed fake data, hack IoT devices completely, cause signal failures or interruption of critical services for the populace. Baig et al. (2017) argue that because of common unencrypted links between sensors, actuators and wireless sensor networks wherein all the communication is transmitted there are severe risks of security lapses.

A reason given for the lack of security measures in IoT devices, Boison et al. (2017) provide, is the reason that in hypercompetitive markets where products are launched daily, the speed of releasing new products with a high convenience factor for customers is essential to stay competitive. In general, security measures have a tendency to cause vexatious or cumbersome extra steps for users and are generally slower to the market because of added complexity (Boison et al., 2017). Also mentioned by Boison et al. is the lack of willingness by consumers/users of IoT devices where they do not have proper incentive to demand higher security.

This is also something that is mentioned by Plachinkova, Vo and Alluhaidan (2016) where they argue that security features often inhibit in the overall satisfaction of usage of devices. This in turn reflects poorly on the vendor / brand which in turn affect sales and competitive advantage. Thibodeaux (2017) reflects upon the same ideas and writes; *“While investment in smart technology has gone up, many of these innovations are deployed without robust testing and cyber security is often neglected.”* Also weighing in on the matter are Sveen, Torres and Sarriegi (2009) who claim that new technology is evolving rapidly and in a speed that makes it difficult for most - even the designers themselves, they mention - to understand, and especially the secure side of it.

Another explanation as to why most IoT devices are generally unsecure stems from the fact that most IoT devices are relatively small and often has a low power consumption, claim Plachinkova, Vo and Alluhaidan (2016). Because of this, additional security features and encryption is hard to implement into the devices. LaBuda and Gillespie (2017) contend that the lack of sufficient security standards for IoT is the main contributor for the overall insecurity of IoT, something also Boison et al. (2017) claim and goes on to suggest that only with a common and shared set of security standards will IoT pose enough secure measure against breaches.

2.3 Cyber security in smart cities

As head of the cyber security department in Swedish Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap, (MSB) Richard Oehme (2017) highlights that with an increase in general digitization, what follows is an increase of vulnerabilities. These vulnerabilities are found in devices, equipment, systems and are constantly on the rise. He writes;

> “*An example of antagonism are cyberattacks aimed toward socially important functions. It happens daily and in great numbers. There are a few examples where antagonists have committed distributed denial of service (DDoS) attacks, with the intention to create interruptions in businesses, theft of information or encrypting information with the purpose to demand ransom.”* (Oehme, 2017)

Kuilboer and Ashrafi (2016), as well as Al-Dairi and Tawalbeh (2017) agree with the sentiment and Al-Dairi and Tawalbeh (2017) argues that with a cumulative increase in digitization in a city, the attack surface follows suit. This stems from the emergent integration of different technologies, systems, networks and more which creates a highly complex, interdependent and communication intense web of digital resources. This in turn is a dangerous phenomenon, Ferraz and Ferraz (2014) points out. They point toward the effect which they call a “Viral effect in urban environment”, which is where an entry point for a hacker gives an opportunity for the malignant actors to reach other, dependent system. They argue that there is a high risk of contamination from the intense and complex communication patterns of an urban smart area. An entry point into one individual system, then, could be used as an entry point toward the smart city constellation of systems in a smart city.

The systems often used in a smart city area is the ones called SCADA, or supervisory control and data acquisition, which are core components in industrial systems (Brenna et al., 2012; Vlacheas et al., 2013; Thibodeaux, 2017). Thibodeaux (2017) highlights SCADA systems as a highly volatile and insecure part in smart cities and argues that if these systems were to be targeted, they could potentially threaten public health and safety and bring a digitised city to a grounding halt. In effect, this creates a problem as SCADA are characteristically insecure and do not feature many cyber security features (Igure, Laughter and Williams, 2006; Munro, 2008; Gold, 2009; Bradbury, 2012; Syed et al., 2017). They are often prevalent in cities where the infrastructure is comparatively old and the smart city initiatives are being implemented in on already existing analogue infrastructure, which is something Syed et al. (2017) contend. They report that industrial control systems of which SCADA systems are apart of, are often antique in today’s rapid technological advancement and therefore lack the proper measures of security that is needed when connected to internet, local networks etc.
They reach the conclusion that there is a severe need for actions to be taken to heighten security in industrial control systems, but contend that the most optimal and secure way would be to entirely scrap decades old systems and implement completely new ones with a more stable and secure architecture.

Considering the complex array of various systems and devices that constitute a smart city, it complicates cyber forensics - that is, the action of investigating and analysing the trail of events that lead to a cyber incident, notably cyber attacks. Baig et al. (2017) claim that this will be and already is a crucial part in a smart city, something that Ferraz and Ferraz (2014) affirm as well. They also insist, however, that as of yet there are still major difficulties in tracing infections and other malicious acts and also the actions for data recovery in smart cities.

In some part, this is because of the issue of hyperconnectivity that John-Green and Watson (2014) emphasize. They state, *“Cyberspace will be a vital component for cities of the future as infrastructures go on-line”* meanwhile reminding us that there are several barriers and difficulties with this, stemming from the four different categories which they divided the engineering risks; *hyperconnectivity*, *messy complexity*, *loss of boundary* as well as *industrialised hacking.* Furthermore, just like Ferraz and Ferraz (2014) claims, there is a lack of analysis tools and techniques available for smart cities to use to mitigate these threats.

Kuilboer and Ashrafi (2016) urges organisations and people to consider cyber security as a pressing matter and claim *"Moving forward without addressing the privacy/security hurdle could derail the safe adoption of the technology."* which is something that also Syed et al. (2017) and Boison et al. (2017) agree with. There is an overall suggestion that cyber security is something that needs to be included at an early stage in projects, regardless of their nature, when it concerns important systems, products and projects.

2.4 Lack of focus on cyber security in smart cities

Even though the fact that cyber security is important has been established; that cyber security is crucial in information heavy environment, cyber security is not one of the primary concerns and considered as a non-challenge in a smart city sphere (Washburn and Sindhu, 2010; Wenge et al., 2014; Pierce and Andersson, 2017). The following section will discuss different reasons for lack of cyber security focus into the category of factors; knowledge and awareness, organizational, financial, outsourcing. The reasons for these categories were that there were common identifiable themes throughout the literature that have plausible effects on the consideration of cyber security. *Knowledge and awareness category* pertains to a more personal level, the perception of individuals, as it is hard to gauge the knowledge and awareness of a complete organisation. The *organisational category* is then used to catch the non-personal factors and pertains to organisation wide decisions, structure and strategy. The *financial category* includes factors related to factors more economical in nature, which could potentially lead to a lack of decisions taken regarding cyber security. Finally, the *outsourcing category* highlights different factors connected with suppliers and contractors.

2.4.1 Knowledge and awareness

Firstly, awareness and knowledge of possible cyber security deficiency is needed in order to impose suitable counteractions. Building a smart city also includes building the foundation for the future systems and integrations describe that a smart city is built in order to improve the quality of life for citizens and that the infrastructure within smart cities need the highest level security in order to secure the smart city objectives (Bartoli et al., 2011; Heo et al. 2014). Furthermore, Wenge et al. (2014) describe cyber security as a key factor for a successful smart city project. Townsend (2013) describes that the digital foundation of smart cities will fail, it is only a matter of when and how much damage it will cause. Thus, the smart city infrastructure needs to include security as a prioritized feature from the beginning, which requires knowledge of smart cities and a long-term perspective.

Smart cities are evolving from innovative technical solutions that create additional security threats and challenges (Chourabi et al., 2012; Elmaghraby and Losavio, 2014). Accessibility, high cost of security applications, privacy of data and threats from hackers, viruses, worms, trojans are some of the smart cities challenges (Chourabi et al., 2012). Smart cities are generally undefended and therefore a target for cyber attacks (Khatoun and Zeadally, 2016). Lack of cyber security testing, lacking security features in devices, poor implementation of security features and out-dated encryption are some of the causes for successful cyber attacks (Khatoun and Zeadally, 2016). IoT devices, which a large amount of smart cities initiatives are built on, faces particularly challenges within security and standardization and scalability, interoperability, reliability are factors to consider (Khan et al. 2012). Pierce and Andersson (2017) elucidate the fact their interviewees did not find cyber security as a hard solved problem. This paper argues that another reason for lack of focus on cyber security is, similarly to what Pierce and Andersson (2017) found, that organisations acknowledge cyber security in smart cities as a non-challenge.

Heo et al. (2014) describe that there are challenges related to the interoperability between devices, which requires a common protocol, and data formats. However, when the systems are built they need to have expandability, which requires planning for future implementations and agreeing to well performing standards (Heo et al., 2014). Goles, White and Diedrich (2005) also note that there exists a lack of awareness of the infrastructures interdependencies as well as the weaknesses. Therefore, interoperability is declared as a challenge for smart cities (Khan et al., 2012; Chourabi et al., 2012) and a failure in the infrastructure put citizens at risk and thus the management of the systems is of utmost importance (Schaffers et al., 2011).

Singh et al. (2013) describe that information security risks should be identified, compared and rated on the severity of the risk in order to explore how the different risks should be approached. In order to identify these risks, Chabinsky (2010) suggests risks analysis to break down the problem into smaller components. The author argues that anyone involved in some kind of cyber security strategy, law, policy or research should complete the so-called *Cyber security Vectors and Risk* framework. Firstly, the organisation needs to explore how an organization can prevent an incident to happen at all; this can include law enforcement, diplomatic or intelligence efforts (Chabinsky, 2010). An organisation can also focus on reducing the vulnerability by security practices, education or more robust security design (Chabinsky, 2010). Lastly, measure should be taken in order to reduce the harm done when the system is breached (Chabinsky, 2010).

In short, this chapter concerning knowledge and awareness describes that:

- When building a smart city to improve the life quality of citizens the digital foundation for future implementations is also built and cyber security should be prioritized from the start, which requires *knowledge* and long-term perspective.
- Firstly, new innovative technical solutions lack standards and create new security challenges that cities need to be *aware* off, when not taken into account leaves smart cities undefended. Secondly, one of these challenges is Interoperability, which requires both planning and *risk awareness* in order to keep systems from failing. Lastly, cyber security risks should be identified and rated in order to create *awareness* and for effective interactions in order to reduce the threat, vulnerability and consequences of a security breach.
- Previous studies presented that cyber security is not considered as a challenge, instead, cyber security is perceived as an matter that will be handled when issues occur, thus, a *non-challenge*.

The identified factors within the category knowledge and awareness: *knowledge*, *risk awareness* and *non-challenge* are included in the theoretical model, coding and further utilized in order to discuss each subcategory in the rest of the research paper.

2.4.2 Organisational

Pearlson and Saunders (2009) highlight the three different domains of an organisation's strategy; organisational, business and information strategy. They argue that success in organisations can only be achieved when the three components are designed into the strategy and supportive of each other. The business strategy is the overall plan for where the business is headed and how it aims to reach there; it's a way to communicate its' goals and is formed as a response to external and internal influences, like market forces, customer demands as well as organisational capabilities. The organisational strategy is a blueprint for the design of the organisation as well as the definitions and how-to's in order to control the organisation's work processes - how the organisation is organised. The organisational strategy forms the way of how the organisation is formed in order to implement its business strategy and how it reaches the business goals. The information strategy comprises the plan of how the organisation uses information services and as organisational strategy tells a story of how its business strategy is implemented.

Pearlson and Saunders continues and mention that when organisations fail to consider information systems strategy when planning business strategy as well as organisational strategy it has a negative effect on the business in one of three ways;

1. The information systems (IS) fail to support business goals
2. IS will fail the organisational systems
3. There will be a misalignment between business and organisational strategy.

Pearlson and Saunders describe strategic alignment when an organisation's business strategy is *"enabled, supported, and unconstrained by technology"*. (Pearlson and Saunders, 2009, p. 24) The thoughts of strategic alignment stems from Henderson and Venkatraman (1993) where they outline the lack of realisation of value from IT investments to a lack of alignment. Both Pearlson and Saunders (2009) and Henderson and Venkatraman (1993) argue that in order for an organisation to achieve an effective business, managers need to have a clear grasp on IT in the organisation; mainly how IS are used and managed.

Pearlson and Saunders (2009) conclude that business strategy is the overall driving factor for both organisational and IS strategy and the organisation and its IS should be both enabling the business strategy. In this research, we extricate the two concepts of aligning business and IT (Business alignment) as well as the alignment of organisation and IT (Organisational alignment) in order to more closely study these factors on focus on cyber security.

To achieve an effective, general information security solution, Kayworth and Whitten (2010) argues that a mix of different factors needs to be focused on. They list an encompassing strategic alignment, a pervasive organisational awareness of information security matters and top management support. These are all heavily pointed toward the more soft values, and not strictly technological actions or focus. Strategic alignment is the key factor, Chen et al. (2008) argues, in order to achieve any success with initiatives with a connection to IT. Johnston and Hale (2009) directly links efficient security through organisational alignment and the utilisation of an information security governance (ISG) in order to achieve strategic alignment. They note that the biggest difference between ISG implementers and non-implementers is the active support of business process owners in an effort of a security culture.

Wang, Ali and Kelly (2015) is in line with these thoughts in regards to handling security issues in smart cities. They conclude there needs to be a more encompassing strategy to handling risks, not merely a technological solution. They divide risks into four different categories;

- One, more technical, that includes system architecture, firewalls and software patches,
- One that concerns softer values, such as malware, security policies and human factors
- Another that includes third-party chains and insider threats
- As well as database schemas and various encryptions available for the organisation.

McFadzean, Ezingeard and Birchall (2007) found that the lack of focus on cyber security in general stems from a lack of knowledge or awareness or simply the top level managers perception of risk, which then creates an individual basis for measures taken to heighten information security by managers. They argue that information security needs to be a board level issue and handled by managers in a structured way, which is something that Kwon et al. (2012), Ma, Schmidt and Pearson (2009) and Johnston and Hale (2009) also agrees with. Sveen, Torres and Sarriegi (2009) also conclude that security management has not been elevated to a strategic level.

When conducting a study with scenario-based tests, Goles, White and Dietrich (2005) found that there was a plentitude of issues with cyber security and gives three critical recommendations. One of these was “*view cyber security as a business issue”* which relates to the board level prioritisation. This is something that Singh et al. (2013) also found, as well as Kayworth and Whitten (2010), who conclude; *“...effective security is achieved holistically through the application of multiple organizational and social alignment mechanisms combined with competence in technology as part of an overall socio-technical strategic focus to information security.”* However, Knapp et al. (2006) found that this is not the case in most organisations and contribute this phenomenon to the lack of top management support and conclude that “*Perhaps an organization’s overall security health can be accurately predicted by asking a single question: Does top management consider security important? If they do not, it is unlikely the rest of the organization will either.”*(Knapp et al., 2006, p. 57). They also note that *“Management frequently does little but pay lip service to security; it is viewed as a cost and a hindrance, not a critical business component.”* (Knapp et al., 2006, p. 54) in bigger organisations. Although in the study, they found that top management support was less of a cited issue in bigger organisations than medium and small sized organisations. Also claimed by the authors is the fact that government move slowly when addressing intricate concepts like cyber security.

Chan and Lin (2007) and Bulgurcu, Cavusoglu and Benbasat (2010) both highlight the need for policies and a pervasive secure practice of technological assets, as they also argue that cyber security is not an issue that is easily solved by merely the use technology. Instead, an organisational alignment between departments and employees is needed. This is something also agreed upon by Siponen, Mahmood and Pahnila (2009) who claims that the visibility and tangibility of security policies affects the employees’ behaviour for policy compliance. This is also confirmed by Doherty, Anastasakis and Fulford (2009) and Puhakainen and Siponen (2010), who emphasizes that non-compliant employees pose serious security risks. Soomro et al. (2016) argue that organisational policies and guidelines has to be established to reach a pervasive cyber security strategy. Also interesting to note is the argument brought forth by Alawadhi et al. (2012) who claim that municipalities and the public sector is not an attractive workplace for IT professionals considering the major upswing in the IT labour market.

In conclusion, the organisational part describes that:

- *Business alignment* is a key factor for successful projects that involve IT. A lack of focus on information security could stem from the top-level managers perception of the risk and needs to be a board level issue. Top management support is needed in order to view cyber security as a business issue.
- *Organisational alignment* is needed in order to achieve a focus and an optimal cyber security. Competence in IT and a social alignment needs to be combined in general projects in order to achieve an effective cyber security.
- The organisation needs *policies* and *training* in order to create awareness and affect employees' behaviour. Compliance of employees in an organisation, regardless of position, is needed.

2.4.3 Financial

Pierce and Andersson (2017) demonstrate the issues in general with cost-benefit analyses of smart city initiatives, which then has a certain effect on something that is not considered as functional in nature - cyber security, that is. Literature already raise the problems of a financial nature (Ferrer et al., 2013; Vilajosana et al., 2013; Manville et al., 2014; Breuer, Walravens and Ballon, 2014) and Ferrer et al. (2013) connects the issue of the risk profile of smart city projects, which is where initiatives such as the Risk Sharing Finance Facility (RSFF) to help fund smart city projects, even with the projected business and economic risk profile. Alawadhi et al. (2012) agree, and also mention insufficient support as a key challenge for smart city initiatives and that there have been several city governments that lost key technology personnel and other cities miss opportunities of updating and upgrading pivotal technical systems for smart cities.

Chourabi et al. (2012) constructed a framework of factors, which, likewise, includes the high cost of IT professionals and consultancies beyond the mentioned factors of high cost of general IT as well as installation and maintenance costs. Soomro, Shah and Ahmed (2016) specifically links the effectiveness of cyber security to top management support, and notes that financial provision is one key deciding factor. This is also something Kayworth and Whitten (2010) points out, that the lack of alignment between security groups or departments as well as business departments often result in budgets not reflecting the need for security financing. This is something that is mirrored in Gordon et al. (2005) where they mention there are several budgeting issues with cyber security measures as well as the existence of an economy of scale phenomenon to cyber security. Rowe and Gallagher (2006) and Alawadhi et al. (2012) also point out that cyber security is a costly investment. Sommestad, Ekstedt and Holm (2013) continue on these thoughts and argue that specialists, experts and consultants in cyber security are costly. In contrast to this, however, Rowe and Gallagher (2006), Alawadhi et al. (2012) and Kuypers, Maillart and Paté-Cornell (2016) mention that cyber security breaches and incidents have costly consequences, where Kuypers, Maillart and Paté-Cornell (2016) not only mention pure financial damage as an outcome, but in conjunction lists business interruption, reputation damage, intellectual property loss and other costs. Notably, it has been proven that a cyber security breach has a tenuous effect on stock prices (Campbell et al., 2003; Kannan, Rees and Sridhar, 2007; Kuypers, Maillart and Paté-Cornell, 2016) which lends support to reputation damage as a severe consequence.

Conclusively, the financial part depicts that:

- There is a general issue with cost-benefit analysis in smart cities and that features that are not direct functions like cyber security can be affected. Cyber security is *costly* and could be an *issue* when prioritising business goals.
- High cost of IT professionals and consultants can be overseen and budgets do not reflect the need of security financing. *Budgets* do not often reflect the need of cyber security.

2.4.4 Outsourcing

Mitton et al. (2012) outlines security as a core feature in devices themselves, instead of an overarching cyber security strategy in smart cities. They highlight that there is a specific lack of homogeneous standards for interoperability between different systems and devices, which they intend on bettering in the suggestion of forming an infrastructure architecture standard for different communication. This is also something mentioned by Al-Hader and Rodzi (2009), where they highlight a need for common and shared architecture by the contractors for smart city initiatives. In relation to this, Elmaghraby and Losavio (2014) write that there is a certain problem that comes with an absence of clear standardised best practice and also relates this to what regulations there is for smart city systems; both best practice as well as the power regulation.

Chabinsky (2010) notes the rapid expanse of purchasing services in a global market, in respect to an organisation’s supply chain, and its’ benefits for rapid invention and innovation as well as lower prices. However, it has also given rise to a higher vulnerability for manipulation, and he specifically mentions computers or architecture that they rely on might already be manipulated or have severe security flaws (Chabinsky, 2010). Furthermore, Gonzalez (2005) describe cyber security as a complex field where the amount of experts is unsaturated, however, only a few organisations have enough resources or motivation to have a full cyber security defence within the organisation. Moreover, it becomes necessary for organisation to outsource cyber security processes (Gonzalez, 2005). Thus, organisations that buy services, products or systems from vendors alternatively contractors rely on their ability to provide sufficient cyber security measures. However, organisations need to carefully consider the decision to outsource cyber security since the decision has both pros and cons, such as loss of control (Khalfan, 2004). Furthermore, an organisation should choose a service provider carefully and evaluate the quality and level of the vendor, considering that the consequences of a security breach will harm the business and possibly create judicial sanctions (Khalfan, 2004). Wenge et al. (2014) and Khalfan (2004) argue that there has to be specific security contracts in order for this vulnerability to be overcome. Furthermore, Khalfan (2004) describe that the contracts need to involve robust provision for cyber security, especially in the service-level agreement. However, the private sector that provides the cyber services are not willing to be responsible or accountable for national security breaches (Carr, 2016). Thus, this paper argues that if governments have problems handling cyber security, local governments probably have the same challenges.

In essence, the outsourcing section outlines that:

- In today’s competitive climate, organisations *trust* their suppliers’ ability to provide sufficient cyber security. However, the private sector is not willing to be held accountable or responsible of national security breaches.
- One way of combating security flaws when buying services or products is by way of extensively developed and comprehensive *contracts* that detail cyber security as a demand.

2.5 Theoretical model

The theoretical model was constructed from the sections 2.4.1 2.4.4 in the literature review, further description of the process is outlined in section 3.2. In the theoretical model four different categories: *knowledge and awareness, organisational, financial* and *outsourcing* are shown the left column, while the 10 factors including descriptions within the categories are represented in the right column.

Table 2.5.1 The Lack Of Focus On Cyber Security Theoretical Model

The Lack Of Focus On Cyber Security Theoretical Model	
Category	**Factors**
Knowledge and Awareness	- *Knowledge*, building a smart city to improve the life quality of citizens the digital foundation for future implementations is also built and cyber security should be prioritized from the start, which requires knowledge and long-term perspective. - *Risk Awareness*, new innovative technical solutions lack standards and create new security challenges that cities need to be aware off, when not taken into account leaves smart cities undefended. Secondly, one of these challenges is Interoperability, which requires both planning and risk awareness in order to keep systems from failing. Lastly, cyber security risks should be identified and rated in order to create awareness and for effective interactions in order to reduce the threat, vulnerability and consequences of a security breach. - *Non-challenge*, cyber security is not considered as a challenge, instead, cyber security is perceived as a matter that will be handled when issues occur.
Organisational	- *Business alignment* is a key factor for successful projects that involve IT. A lack of focus on information security could stem from the top-level managers perception of the risk and needs to be a board level issue. Top management support is needed in order to view cyber security as a business issue. - *Organisational alignment* is needed in order to achieve a focus and an optimal cyber security. Competence in IT and a social

	alignment needs to be combined in general projects in order to achieve an effective cyber security. - *Policies* and *training* are needed in order to create awareness and affect employees' behaviour. Compliance of employees in an organisation, regardless of position, is needed.
Financial	- *Cost Issue*, there exists a general issue with cost-benefit analysis in smart cities and that features that are not direct functions like cyber security can be affected. Cyber security is costly and could be an issue when prioritising business goals. - *Not in budget*, high cost of IT professionals and consultants can be overseen and budgets do not reflect the need of security financing. Budgets do not often reflect the need of cyber security.
Outsourcing	- *Trust*, in today's competitive climate, organisations rely on suppliers' ability to provide sufficient cyber security. However, the private sector is not willing to be held accountable or responsible of national security breaches. - *Contracts*, a way of combating security flaws when buying services or products is by way of extensively developed and comprehensive contracts that detail cyber security as a demand.

3 Research method

In order to deepen the knowledge about the reasons for lack of focus on cyber security in smart city initiatives this paper explores smart cities, cyber security and factors that can explain why smart city project managers, coordinators and leaders do not consider cyber security as a challenge. In order to validate replicability of this paper, the methodological path for gathering literature for the literature review and the empirical data gathering process is described in detail in this part of the paper. Firstly, we present how the literature used in this paper was gathered (see 3.1). Secondly, the research design choice is described and motivated. Thirdly, the selected informants and their criteria is motivated, as well as the interview structure and the pilot interview. Next, the data analysis procedure for the empirical results is described, and lastly, research quality and ethical aspects of the paper are discussed.

3.1 Literature collection

The key words used to find the literature were: smart cities, smart city, cyber security, technology, digitalisation, Internet of things, IoT or a combination of these. In order to gain a better understanding of the smart city initiatives in Sweden we could also explore the different municipalities websites and deepen our knowledge of city digitalization in a near environment.

First and foremost a vast amount of literature was reviewed in order to gain an understanding of both cyber security, smart cities as well as the interrelationship between the concepts. A comprehensive literature review is a needed foundation in order to find potential gaps or appropriate research problems. Bartunek et al. (2006) describe that by increasing the amount of effort into research, it has a direct causal effect on the level of interest. Therefore, for our research we chose a subject that we are genuinely interested in which we believe is the bedrock of interesting research. In order to find interesting papers on the subject we primarily search in the so-called basket of eight. The basket of eight are the eight top management information systems journals that are selected by the Association of Information Systems and focus on behavioural and business oriented IS research. These journals are appropriate for our research field and education but are also peer reviewed and highly regarded in the IS community as a whole. Furthermore, the search engine LUBsearch provided by Lund University as well as Google Scholar was used to find additional literature. When using a source that was not included in the basket of eight, we utilized the Norwegian list to confirm the validation of the source; anything that did not have rank 1 was not included.

Table 3.1.1 presents the final result of the literature review that could explain reasons why cities tend to not prioritise cyber security grouped into the different categories *knowledge and awareness, organisational, financial* and *outsourcing*. The justification of the different factors was previously explained in chapter 2.4.

Table 3.1.1 Category Model

Category Model	
Knowledge and Awareness	[Chourabi et al., 2012; Chabinsky, 2010; Elmaghraby and Losavio, 2014; Goles, White and Diedrich, 2005; Heo et al., 2014; Johnston and Hale, 2009; Khan et al., 2012; Schaffers et al., 2011; Singh et al., 2013; Townsend, 2013; Wenge et al., 2014]
Organisational	[Bulgurcu, Cavusoglu and Benbasat, 2010; Chabinsky, 2010; Chang and Lin, 2007;Chen et al., 2008; Doherty, Anastasakis and Fulford, 2009; Goles, White and Dietrich, 2005; Johnston and Hale, 2009; Kayworth and Whitten, 2010; Knapp et al., 2006; Kwon et al., 2012; Ma, Schmidt, & Pearson, 2009; McFadzean, Ezingeard and Birchall, 2007; Puhakainen and Siponen, 2010; Singh et al., 2013; Siponen, Mahmood and Pahnila, 2009; Wang, Ali and Kelly, 2015]
Financial	[Alawadhi et al., 2012; Breuer, Walravens and Ballon, 2014; Campbell et al., 2003; Chabinsky, 2010; Chourabi et al., 2012; Ferrer et al., 2013; Gordon et al., 2005; Kannan, Rees and Sridhar, 2007; Kuypers, Maillart and Paté-Cornell, 2016; Kayworth and Whitten, 2010; Manville et al., 2014; Sommestad, Ekstedt and Holm, 2013; Soomro, Shah and Ahmed, 2016; Vilajosana et al., 2013]
Outsourcing	[Carr, 2016; Chourabi et al, 2012; Chabinsky, 2010; Khalfan, 2004; Mitton et al., 2012; Wenge et al., 2014;]

3.2 Developing the theoretical model

As previously outlined, the research paper sets to describe the reasons for the lack of focus in cyber security in smart cities. Previous literature does not describe factors that explain why cyber security is not regarded in a smart city context; however, common reasons for other settings are explained. Thus, this paper needed theoretical guidance in order to answer the research question.

The previously described Category Model (table 3.1.1) the reasons found in the literature review was grouped into the different categories *knowledge and awareness*, *organisational*, *financial* and *outsourcing*. Furthermore, the factors within each category that could explain smart cities lack of focus were identified which resulted in a list of factors. However, a lot of the listed factors were overlapping or phrased differently and in the end the initial factors were aggregated into 10 problem factors, *knowledge*, *risk awareness*, *non-challenge*, *business*

alignment, organisational alignment, policies and training, cost issue, not in budget, trust and *contracts.*
The process of identifying the factors within a category is presented below.

To extract summarizing data from the literature review, a table was formed in order to give an easy and understandable structure of the literature used for the categories. The category then lists corresponding references, which discuss this topic. An extract of this can be seen in the following table 3.2.1.

Table 3.2.1: Extract from the category framework from 3.1

Categories for lack of focus on cyber security	
Organisational	[Bulgurcu, Cavusoglu and Benbasat, 2010; Chabinsky, 2010; Chang and Lin, 2007;Chen et al., 2008; Doherty, Anastasakis and Fulford, 2009; Goles, White and Dietrich, 2005; Johnston and Hale, 2009; Kayworth and Whitten, 2010; Knapp et al., 2006; Kwon et al., 2012; Ma, Schmidt, & Pearson, 2009; McFadzean, Ezingeard and Birchall, 2007; Singh et al., 2013; Siponen, Mahmood and Pahnila, 2009; Puhakainen and Siponen, 2010; Wang, Ali and Kelly, 2015]

The table 3.2.1 then gave rise to a more summarizing and concluding table, named the *The Lack of Focus on Cyber Security Theoretical Model*, which briefly explains the different factors in that category. An example of this can be found in table 3.2.2

Table 3.2.2. Extract from the theoretical model

The Lack Of Focus On Cyber Security Theoretical Model	
Category	**Factors**
Organisational	- *Business alignment* is a key factor for successful projects that involve IT. A lack of focus on information security could stem from the top-level managers perception of the risk and needs to be a board level issue. Top management support is needed in order to view cyber security as a business issue. - *Organisational alignment* is needed in order to achieve a focus and an optimal cyber security. Competence in IT and a social alignment needs to be combined in general projects in order to achieve an effective cyber security. - *Policies* and *training* are needed in order to create awareness and affect employees’ behaviour. Compliance of employees in an organisation, regardless of position, is needed.

3.3 Research design

The aim of this study was to acquire a deeper understanding as to why decision makers in smart city initiatives do not usually focus on cyber security. Due to this, the chosen method for the study was qualitative because of the rather unexplored research area of these two key concepts combined, “smart city and cyber security”. The approach was also interpretivist in its nature because of the potential to better gain an understanding of practitioners’ perspective (Orlikowski and Baroudi, 1991; Gummesson, 2003; Bhattacherjee, 2012).

The research field is a multifaceted topic due to the combination of two highly complex topics by themselves. Cyber security has a varying degree of intricacy owing to its interdisciplinary background consisting of perspectives of organisational, behavioural science, technological, business science and more. Similarly, the research field of smart city combines a variety of research fields into one interdisciplinary field, including scientific fields of sustainability, organisation, information science and more. Heightening the complexity of the research area is the wide variety of practional actors.

Considering the multifaceted topic that “smart city cyber security” is, the interpretivist approach was positive for its viability of gaining an understanding from the perspective of our research subjects by embracing their various experiences (Orlikowski and Baroudi, 1991; Gummesson, 2003; Bhattacherjee, 2012)

Within the qualitative data collection method, Recker (2013) mentions that an interview is the most prominent method. The outline for the data collection in this study is *descriptive interviews*, where Recker argues descriptive interviews has a high potential for describing phenomena as perceived by the interview subjects. The aim of the study is to rationalise the thoughts and perceived notions about cyber security in smart cities and infer a deeper knowledge as to why cyber security might not be a prioritised area of smart cities. Considering our aim to rationalise the focus of decision makers in smart cities, interviews is an excellent way to gather data, Bhattacherjee (2012) argues, as it could create a potentially intriguing narrative.

The chain of evidence, as can be explored in the previous chapter, started from the conducted literature review from which a brief theoretical model was created. The theoretical model lead to the creation of an interview guide with questions corresponding to common themes throughout the varying literature.

3.4 Informant selection

The selection of informants was a process of which began with a sampling of case cities based on two criteria, namely the city has to;

- Be within the European Union
- And actively pursuing smart city projects / has previously pursued and implemented smart city initiatives

The aim of the sampling was to have a geographical spread and to give further depth within the given time of conducting the study. This is because a range of cases serves as a strengthening action for the results, and benefits pattern matching and the robustness of the study (Recker, 2012). We explicitly chose the cities that were undertaking or had undertaken previously projects in the area of smart cities.

Our criteria of the smart city being European stems from the fact that there are several initiatives on a European level concerning smart cities, including *EU-Gugle* (eu-gugle.eu) and *Step Up Smart Cities* (stepupsmartcities.eu). Many smart city projects are also funded by various European Union programmes, such as Horizon 2020 (Papa, Gargiulo and Galderisi, 2013; ec.europa.eu/inea) and there are initiatives designed to assist cities in their smart city endeavours, with the European Commission's Strategic Energy Technologies Information System (SETIS) European Initiative on Smart Cities (Marsal-Llacuna, Colomer-Llinàs and Meléndez-Frigola, 2015; setis.ec.europa.eu) being one of these. In effect, all of these different factors have an impact on the smart cities and are likely to share a set of commonly used standards within technology, legislation and more, which creates a stronger comparative foundation for our study.

Examples of lists that were used to find the case cities in Europe were different federations or coalitions for smart city initiatives. One of these was Smart City Sweden who explain that they are a "... national export and import platform for smart and sustainable city solutions." (www.smartcitysweden.com) Provided was a multitude of reference cases within various "focus areas" ranging from *smart waste management*, *smart mobility* and more and which cities were featured. This gave us an understanding of which cities were partaking in smart city projects. Another list of smart cities was the one featured in the Grow Smarter initiative, which also featured reference cases. We were also assisted by the study conducted by Caragliu, Bo and Nijkamp (2011), which gives an overview of different smart cities in Europe. In table 3.4.1, an overview of the different cities selected is shown.

Table 3.4.1 Smart Cities Sampling

Smart Cities Sampling	
City	**Country**
Aalborg	Denmark
Aarhus	Denmark
Copenhagen	Denmark
Odense	Denmark
Helsinki	Finland
Turku	Finland
Cork	Ireland
Amsterdam	Netherlands
Rotterdam	Netherlands
The Hague	Netherlands
Utrecht	Netherlands
Oslo	Norway
Gothenburg	Sweden
Helsingborg	Sweden
Jönköping	Sweden
Lund	Sweden
Malmö	Sweden
Stockholm	Sweden
Umeå	Sweden
Uppsala	Sweden
Örebro	Sweden
Liverpool	United Kingdom
London	United Kingdom
Manchester	United Kingdom

3.4.1 Selection of interview subjects

Once a selection of a wide range of cities was made, what followed was a standard approach to contact the different cities with a mail for further contact details. The mail followed a standard outline with a brief introduction of ourselves followed by a brief of the topic of the interview. To be able to find a corresponding theme throughout our interviews, the focus was on interviewing with an overarching view of the details of smart city projects taken within the city or decision makers themselves. The mails also provided a few of the roles we were interested in interviewing, namely; project manager, city planning manager, city manager and coordinator. Due to the role's pervasive but at the same time vague nature, the title of our interview subjects is at times hard to define exactly. Instead, we gave, as mentioned above, a brief overview of the interviewee's responsibilities we intended to interview. In table 3.4.1.1, an overview of the interview subjects can be found.

Table 3.4.1.1 Overview of participants in the study

Overview of participants in the study				
#	**City**	**Role**	**Date**	**Duration**
1 (Pilot)	Malmö	IT architect	2018-05-03	55:36
2	Umeå	Strategic development coordinator	2018-05-03	48:58
3	Stockholm	Head of Department / Coordinator	2018-05-03	31:02
4	Stockholm	Project leader for digitalisation	2018-05-04	35:45
5	Jönköping	Project manager mobility management	2018-05-04	44:13
6	Aarhus	Smart city project lead	2018-05-09	37:01

3.4.2 Language used in interviews

Due to initial issues in finding willing participants at an early stage of our research, we decided to try contact municipalities and cities in Sweden in Swedish in an assumption there was a slight unwillingness of participating in English. The second attempt was received in a better light and participants were found with more ease. Because of this, most interviews have been conducted in Swedish and the quotes, which are used in the empirical results section, were translated with meticulousness. There were no language barriers present and with our backgrounds as researchers and experience in academic English, it was not considered as a problem when analysing the interviews and translating coded parts into English for the reader's understanding.

3.5 Interview structure

The interviews have been conducted as semi-structured or unstructured interviews (Bhattacherjee, 2012) because of the need to further explore the unknown themes that might arise from the interviews. Kvale (2006) argues that the interview method is beneficial for relatively unexplored fields lacking established theories. As mentioned in 3.1, the interviews were based on an interview guide or protocol. The interview guide served as the basic outline for the interviews, which then gave an opportunity to adapt and deviate from in the sense of follow-up questions depending on the answers given by the informant. The semi-structured interview method is beneficial for this matter as well as correlational questions, which was beneficial for a deeper understanding, especially considering the relatively unexplored area of our research.

The interview was composed of both close-ended and open-ended questions, where the potential of a semi-structured interview gave the researchers an opportunity to create follow-up questions to the answers of the close-ended questions for further details. Bhattacherjee (2012) mentions that probing questions even if these are not in the protocol is necessary to provide qualitative data. Recker (2013) also argues that interview questions need to be simple in usage of technical words and without any jargon to ensure an understandable tone and language.

3.5.1 Interview Conduct

By the guidelines offered by Bhattacherjee (2012), interviews were conducted with a confident tone and were readily booked in advance to avoid confusion. A brief overview of the study was given by the researchers ahead of time and also explained ahead of the actual interview in a succinct manner. Measures were taken to explain the offer of confidential data ahead of the actual interview and the participation was asked yet again before the interview was started.

No questions were excluded and the order of the questions was followed, in order to fulfil a rigorous interview process. The interview followed the structure of the script with it deviating when follow-up questions were posed for further clarification or bidirectional understanding of relatable topics. Bhattacherjee (2012) highlights follow-up questions as beneficial for contextual understanding and further understanding of correlations between constructs. Probing techniques offered by Bhattacherjee (2012) were used for this manner. The researchers used neither a wholly disapproving nor approving tone during the interviews to focus on the experience of the interviewee.

3.5.2 Interview questions

From the different categories of factors, some questions were proper to ask considering the red threads that could be found in the literature. These questions are meant to explore each category of factors individually and try to distinguish the most deciding factors for the lack of focus on cyber security in smart city projects. The questions can be found in the following table categorised in five different categories as well as the corresponding source.

Table 3.5.2.1 General Questions

General Questions			
Category	**Question**	**Described**	**Source**
General	Do you experience that in the smart city initiatives in your city, there is sufficient focus regarding cyber security?	Section 2.4	Pierce and Andersson (2017) Wenge et al. (2014) Washburn and Sindhu (2010)

The general question was an endeavour to hone the participant's attention to the area and start slowly with an overarching question, which pertains to our research area. This enabled us to have a background for our participant's answers about the general experience regarding cyber security in the respective cities and the smart city initiatives.

Table 3.5.2.2: Knowledge and awareness questions

Knowledge and awareness questions		
Category	**Question**	**Source**
Knowledge & Awareness Described in section 2.4.1	What possible risks of smart city initiatives do you see?	Chourabi et al. (2012) Elmaghraby and Losavio (2014) Townsend (2013)
	Do you follow any security standards when implementing smart city projects?	Wenge et al. (2014) Khan et al. (2012)
	Do you conduct any risk analysis when considering smart city projects?	Chabinsky (2010) Singh et al. (2013)
	When considering interconnectedness / interoperability, do you consider security flaws?	Heo et al. (2014) Schaffers et al. (2011) Khan et al. (2012) Chourabi et al. (2012) Goles, White and Diedrich (2005)
	Do you have any employees working with cyber security in smart city initiatives?	Chourabi et al. (2012) Johnston and Hale (2009)

With the questions regarding awareness and knowledge the aim was to research the perception of our participants and explore the concepts together with our participants pertaining to cyber security in the smart city projects.

Table 3.5.2.3: Organisational questions

Organisational questions		
Category	**Question**	**Source**
Organisational Described in section 2.4.2	Do you have overarching cyber security strategy?	McFadzean, Ezingeard and Birchall (2007) Kayworth and Whitten (2010) Wang, Ali and Kelly (2015) Puhakainen and Siponen (2010) Ma, Schmidt and Pearson (2009) Singh et al. (2013)
	Is cyber security considered when discussing new strategies or new projects?	Chen et al. (2008) Johnston and Hale (2009) McFadzean, Ezingeard and Birchall (2007) Kayworth and Whitten (2010), McFadzean, Ezingeard and Birchall (2007) Wang, Ali and Kelly (2015) Kwon et al. (2012)
	Is cyber security seen as an overall business security issue?	Goles, White and Dietrich (2005) Kayworth and Whitten (2010) Kwon et al. (2012) Chabinsky (2010) Wang, Ali and Kelly (2015)
	Are there cyber security policies and/or projects for creating user awareness and training within your organisation?	Knapp et al. (2006) Ma, Schmidt and Pearson (2009) Johnston and Hale (2009) Chang and Lin (2007) Ma, Schmidt and Pearson, (2009) Singh et al. (2013) Siponen, Mahmood and Pahnila (2009) Doherty, Anastasakis and Fulford (2009) Puhakainen and Siponen (2010) Bulgurcu, Cavusoglu and Benbasat (2010)

The questions concerning organisational factors were meant to explore the organisational perception of cyber security and what existed in the organisation in terms of strategies, policies and alignment in relation to cyber security.

Table 3.5.2.4: Financial questions

Financial questions		
Category	**Question**	**Source**
Financial Described in section 2.4.3	Do you budget for cyber security? Specifically in smart city projects?	Soomro, Shah and Ahmed (2016) Kayworth and Whitten (2010) Alawadhi et al. (2012) Gordon et al. (2005)
	Is the cost an issue when considering cyber security measures? Do you feel enough money is being spent on cyber security?	Chourabi et al. (2012) Gordon et al. (2005) Alawadhi et al. (2012) Chabinsky (2010)
	What percentage do you consider you spend on pure cyber security measures?	Gordon et al. (2005)

The aim with the questions regarding financial factors was to explore the participants' experiences with costs and budgets in correlation to cyber security measures.

Table 3.5.2.5: Outsourcing questions

Outsourcing questions		
Category	**Question**	**Source**
Outsourcing Described in section 2.4.4	How much trust do you put on suppliers/contractors on their security?	Carr (2016) Chabinsky (2010) Khalfan (2004) Mitton et al. (2012)
	Do your SLAs feature cyber security as a factor?	Chabinsky (2010) Chourabi et al. (2012) Wenge et al. (2014) Khalfan (2004)

The questions regarding outsourcing were meant to explore how much of cyber security was left upon the suppliers/contractors and therefore may affect the considerations given to it in a project.

3.6 Pilot interview

A pilot interview was held in order to assure the quality of the script (Bhattacherjee, 2012). The act of pilot testing is extremely important, Bhattacherjee notes, as it highlights flaws or potential problems in the instrumentation or research design. This was done by way of interviewing an expert practitioner in a smart city context. The goal was to examine and evaluate the structure, questions and the clarity of the questions to the interviewees. We were also interested in ascertain the level of motivational factor for the interviewees to further elaborate answers. The pilot interview offered an opportunity to conduct an evaluation for optimal collection of rich data. The pilot testing was held on Skype, just as the others were meant to be as well, in order to test the script in its' intended manner. The wording of questions was slightly changed and introduction to our concepts was given before asking if the interview could be recorded.

3.7 Data analysis

The interviews were conducted by Skype and recorded with software. The interviewees were asked for consent for recording beforehand in line with ethical considerations. The interviews were then transcribed verbatim in accordance with principle of accuracy of data. The text was then analysed by intense scrutiny as the result of the analysis is highly dependent on the researchers (Bhattacherjee, 2012). The aim of the qualitative analysis understands a phenomenon, Bhattacherjee mentions, which then lends itself handily for our research question.

An open coding was conducted as per Bhattacherjee's (2012) guidelines and be done with an open mind without any pre-existing expectations or biases. Corbin and Strauss (1990) also highlight the use of open coding, with its' potential of using corresponding themes throughout interviews, and how it could be applied. With the use of the open coding method we found common themes, events, ideas and coded as concepts in the raw data. To ensure optimal coding, coding was done separately by both researchers and then matched by combining the two transcriptions for further accuracy and rigour by complementing the results of the open coding (Bhattacherjee, 2012). The concept of "cross-checking" facts, which is also detailed by Bhattacherjee, was followed, and similar concepts and patterns were analysed ignoring contextual differences to prevent idiosyncratic conclusions (Bhattacherjee, 2012). The aim was to develop a more inclusive and generalizable study, in the goal of a higher transferability (Recker, 2013).

After the open coding was conducted we turned to coding in themes in order to find relationships as help to explain the phenomenon and correlate data found. This was used to analyse interpretively, as per Bhattacherjee's (2012) guidelines, in order to provide a narrative of the phenomenon that can explain and communicate the reasons behind the way participants acted the way they did. The researchers conducted this in a method of recurrent, intense debating sessions.

The way the coding was done was a loose way of combination of following the concepts of *a priori* and *grounded* coding, which is one of the most common ways of coding, according to Stuckey (2015) and detailed in Fereday and Muir-Cochrane (2006) as *inductive* and *deductive* coding hybrid. Mostly, this followed the way of having concepts that were ordained in previously established theoretical model and then concepts found that were not included in these models.

Table 3.7.1. Codes that were used analysing the data

Codes that were used analysing the data		
Category	**Factor**	**Code**
Knowledge & Awareness	Risk Awareness	K&A-RA
	Knowledge	K&A-K
	Non-challenge	K&A-NC
Organisational	Business Alignment	O-BA
	Organisational Alignment	O-OA
	Policies and Training	O-PT
Financial	Cost Issue	F-CI
	Not in Budget	F-NB
Outsourcing	Trust	OS-T
	Contracts	OS-C
Other Inputs		OI

3.8 Research quality

For an optimal degree of rigour and high research quality, general guidelines, principles and recommendations were followed. Multiple case cities were chosen and interviews were chosen with practitioners with analogous responsibilities to achieve triangulation in the data collected (Hevner and Chatterjee, 2010; Recker, 2013). The interview guidelines provided by Recker (2013) and Bhattacherjee (2012) were adhered to, for a higher quality of research. Furthermore, the script was pilot tested (Bhattacherjee, 2012) and improved upon as a consequence. In order to achieve a higher reliability and quality coding, coding was done separately and compared in sessions (Bhattacherjee, 2012; Recker, 2013). In essence, dependability was achieved in the cross-checking and the structured coding, credibility by way of transcriptions and triangulation, conformability by way of structured interviews with different hypotheses as well as transferability by choosing several different cities and rich, detailed descriptions of the research contexts (Bhattacherjee, 2012; Recker, 2013)

A member check was also conducted throughout the interview process in order to validate our data, as Krefting (1991) outlines as a technique of increasing rigour. Informants were informed of specific and integral concepts of our study beforehand and after transcription was done, a copy of the transcription was sent to the participants in order to decrease the chance of misrepresentation, in line with Krefting's (1991) writings.

3.9 Research ethics

To ensure an ethical research, the guidelines provided by Recker (2013) were followed throughout the research. The four rules of ethicality, responsibility, accountability, liability and due process was adhered to. The right to anonymised data, or confidentiality of the data, was given to our participants to ensure an ethical data collection and utilisation of said data in the research.

Also important was the right of voluntary participation of the interviewees. The first question about this started in the initial contact but was also repeated before the interviews as well as the right of consent to being recorded. Participants were informed of known potential risks. As the result of this study will be made public, participants were also informed of this fact (Brinkmann and Kvale, 2005). Considering the public nature of our participants (working in municipalities and in the public sector), there were minor complications of this.

The data was then stored with secure procedures and require proper login information to access and will be erased as soon as the need of use of said data is terminated. Ethical obligations of honesty and complete reporting were followed strictly and transcriptions were done verbatim to the best of our capabilities as researchers. When doing the interpretive analysis, the researchers play a crucial part in the discernment of meaning from the collected data, as the core is that knowledge of reality stems from human actors and knowledge is a constructed concept (Walsham, 2006).

Regarding the ethical issues in writing that Recker (2013) mentions, measures were taken to conduct the research according to principles. Correct referencing to combat plagiarism was followed by structure of the Harvard Style for Lusem. Also considered was the ethical framework for information systems researchers (Bhattacherjee, 2012; Recker, 2013), which was integrated into our conduct throughout the entire research process as a mind-set.

4 Empirical results

This chapter will present the results from the interviews. The results are divided into different sections, which are based on the framework and subcategories based on the coding. The reason for this is to facilitate reading and have a pedagogical structure for easier understanding of the data.

4.1 Knowledge and awareness

A main theme of the literature review was that a lack of knowledge and awareness of security risks in smart cities could be reasons for lack of focus on cyber security. This part will describe the interviews answers to the questions regarding knowledge, risks of implementing smart city solutions as well as if it is a non-challenge.

4.1.1 Risk awareness

The literature describe that a common reason for lack of emphasis on cyber security is dependent on the top managers perception of the risk. Therefore, this part of the paper describes the interviewees' answers regarding their awareness of the possible risks that can oppose a threat for smart cities.

Interviewee 2 states that there are cyber security risks of smart cities and smart city initiatives, but is unable to describe specific risks (IP2:5) or the general threat against smart cities (IP2:7), however, the organisation as a whole prioritises handling these risks (IP2:5). Furthermore, the risk analysis is grounded on the requirements of the EU-commission which funds the projects and a specific cyber security risk analysis is not conducted (IP2:13). More or less interviewee 2 described that smart city projects is handled in the same way as other city projects and follows the same structure and similar projects in the city (IP2:13).

"To be perfectly candid, smart city projects is to great extent just like our ordinary projects, there is no difference. We see ourselves as a smart city, with our strengths and weaknesses…"
IP2:13

Interviewee 3 divides the risks in three categories when asked if he experiences any threats toward smart city initiatives but mentions privacy and personal integrity foremost (IP3:17). The other two categories he mentions is the security with losing information and the recovery of data and systems and the third is systematic errors in collection of data.
He argues that data collection in some level has been conducted for a long time and that there is no difference between now and in the past and merely mentions that there is a larger quantity of data. He notes:
"In reality, there is no difference now in regards to earlier, it's just that we are gathering more data now because it's easier to collect it and also easier to put in controls. There are both problems and possibilities." (IP3:17)

Interviewee 4 sees no real threats concerning smart cities as of this moment. IP4 mentions that they are trying to plan ahead for the journey of smart city Stockholm and mentions they are trying to establish an ethics council in order to "do right" (IP4:8) which includes representatives from different departments in the city.

Interviewee 5 recognised the privacy issues when specifically asked about the perception of cyber and information security risks, and mentioned that the privacy and personal data is the thing to protect. IP5 highlighted GDPR in this matter and argued that the highest priority is making sure that the organisation does not break any rules or laws.
"Well, privacy has to be the one, the thing to think about and how to secure it in various ways. We are already faced with this today because of GDPR. No, there's something - that's the real big part. That we simply do not break any rules or laws." (IP5:15)
When specifically prodded about any threats IP5 acknowledged that this is a matter that is more important when the smart parts of a city is more in control (IP:17) but did not acknowledge any plans regarding any strategy for the future. IP5 did not recognise any major threats;

"For our part the risks are maybe not that big. We are not involved in that (smart parts that control physical infrastructure) yet, that's a lot of operation that's about. We're looking at more behavioural change and things like that, and there, I don't know, if someone were to feed data into some apps or something similar that people are going to take the car instead of taking the bike, that's not what we want, really, but it's no catastrophe if someone would do that, so to say." (IP5:17)

IP5 was not certain if there are any risk analyses done in the regard of cyber security in any of the previous projects or if that is part of the procedure.

Interviewee 6 highlighted a dilemma between creating better services, not surveilling citizens and creating secure solutions, however, the interviewee do not think that the smart city projects affect any crucial infrastructure yet. Therefore, there has not been any discussion about protecting human lives (IP6:5). Furthermore, IP6 described that the digitizing of services leads to more vulnerability but not to the point where it threatens people's lives, at least not yet (IP6:7). IP6 also illuminated that fact that organisations may need some kind of accident in order to focus on cyber security risk analysis and measures (IP6:34).

"We haven't had any accidents since the big one in 2014. But I mean, sometimes it takes something like that for the attention on it to be sharpened, again."
(IP6:34)

Lastly, IP6 described that smart cities is the next step and with new technology solutions and innovations comes bigger risks (IP6:34).

4.1.2 Knowledge

This section describes the interviewees' answers regarding their own knowledge of cyber security in smart cities.

Interviewee 2 deflected a few questions but was generally aware to some degree of the problems and risks of interoperability of smart cities. However, the main focus here was instead personal integrity and the point of cyber security was not a heavily focused one. IP2 was more informed, both internally within the organisation, but also externally, the overarching chain of communicating personal data. (IP2:21). IP2 describes that there exists an IT-strategy, however, knowledge of what it consists of is lacking (IP2:53).

Interviewee 3 was rather sceptical toward a complete connected society and that a connected infrastructure communicating with everything was a “dream for engineers”. (IP3:27) He mentions an example of smart lamp posts that light up when humans approach and the complexity of there already being four different systems for this available from vendors and recognised there were ‘problems’ with this but didn’t know the specifics. He did not acknowledge any cyber security flaws or risks with it and instead mentioned that it’s something that needs to be worked upon in the future, with further procurement. IP3 recognises no risks with a more connected infrastructure with higher interoperability and instead focuses on the problems of reaching an optimal interoperability between different parts. (IP3:29)

Interviewee 4 had a rather comprehensive knowledge of cyber security in smart cities, however, IP4 lacked knowledge of the security standards in the city. Furthermore, IP4 describe that a person with knowledge about cyber security is present throughout the projects (IP4:11).

Interviewee 5 was generally a bit uncertain what parts of cyber security detailed into the daily work and instead focused more on the privacy matter (IP5:4). There were few mentions of the more cyber security aspects, even with explanations and further reminders of what it entailed earlier on in the interview. Even though some information was given for projects, deflections were made as well when it came to cyber security matters (IP5:9). Also done in IP5:19, he refers to others when he says he is not involved in cyber security matters. When it came to the overarching cyber security strategy he was rather uncertain as to what existed (IP5:21) but mentioned “I would assume it was so, but I’m afraid to give a direct answer.” (IP5:21). He gives this assumption once again pertaining to cyber security as overall business risks; “My feeling is that yes, that (cyber security) has to be a catch-all security matter.” (IP5:33). IP5 recognises some issues with interoperability and brings to light an example of protection of information - personal data - where they have worked with an external actor. He mentions that when it comes to the delivery to external actors he has faith in the IT-department who are responsible for the direct communication and delivery of personal data. He does, however, admit that he is not aware of an increase in security flaws when it comes to delivery of information to external actors and instead directs us to someone else in the organisation. (IP5:25)

4.1.3 Non-challenge

Interviewee 2 had already stated that there are cyber security risks and especially so when the ambitions for smart cities arise. Even though IP2 recognises the risks and problems concerning cyber security, he states that there had been no real threat and neither recognises or states that the threats might continue in the future. Also expressed is that the solutions come as an answer to a problem and how they work. *“I have no reason for, there has been nothing so far* *that we feel - that the cyber security has been challenged so far. Nothing that I know of, any way."* (IP2:37) His experience is that instead the focus has been on other things and used the example of Ruggedised smart city project, that cyber security is in parts included, but the focus had instead been upon the deliverable. (IP2:41).

Interviewee 3 acknowledged cyber security risks and problems but instead prioritised other risks instead of cyber security on separate and multiple occasions. (IP3:25, 27, 42, 50) When asked about the budget and if cyber security was budgeted specifically, IP3 said: *"Not more than what I have described earlier. That information security is a part of it, but there are many other risks that we consider are bigger and more comprising. In projects like these, we receive 25 million euros, that is to say quarter of a billion for the project and then it's the matter of making sure that the project goes smoothly and reaches the end, so we get the financing that was considered, so it's a big economical risk that we handle in projects like these. It's very important to handle time plans and get past potential delays and so on."* (IP3:42) He also acknowledged that cyber security has not been featured in the top during risk analyses (IP3:50). Another quote later on during the interview was also of note: "In these contracts it's very important to, that those risks that we see are vastly more than cyber security." (IP3:64)

Interviewee 6 describes that other companies focuses on cyber security and puts it high on their agenda, however, cyber security is not a major issues for their organisation (IP6:47). Instead, focus is shifted towards the present challenges of the city and how it could be solved with technology (IP6:36)

"I mean, some companies of course have it very high on their agenda because they need to. But it is not something that is a major issue for us."
(IP6:47)

4.1.4 Summary – knowledge and awareness

In regard to risk awareness three of the respondents acknowledged that there could be threats in the future, however, in the present there are not any real threats. One respondent knew that risks exists but could not be specific and another respondent described that there is no difference between pre and post smart city initiatives, it is just a larger amount of data. Another interesting answer described that smart city projects do not affect critical infrastructure but when it does, more risks will come.

Three of the respondents had some knowledge about how cyber security was dealt with in the city. However, the privacy aspect was being prioritized rather than cyber security. The knowledge about cyber security in smart cities differed quite drastically where one respondent had a comprehensive knowledge and one respondent viewed a connected infrastructure as not probable and did not acknowledge any cyber security flaws or risks in smart cities.

Three of the respondents stated that cyber security is not a major issue for their cities.
One respondent described cyber security is not a major issues, the issue is how to solve challenges with technology. Another respondent described that they have not had any problems so far and that the focus is rather on the deliverable mentioned that in the contracts, there are other risks that are vastly more important than cyber security.

4.2 Organisational

Another reason for lacking focus on cyber security is the organisational factors. Business strategic alignment is crucial and cyber security needs to be viewed as a business issue and not merely a technology issue. Therefore, the organisation needs to acknowledge and include cyber security in an early stage of planning and included in overall business risks. This part of the paper describes the interviewees' answers regarding the organisational factors, business strategic alignment, organisational alignment and policies.

4.2.1 Business alignment

Interviewee 2 described that there is not, to the interviewees knowledge an overarching strategy of cyber security (IP2:45). Furthermore, IP2 describes that the IT-department should be able to give more accurate answers (IP2:45). In a later stage of the interview IP2 explains that the IT-department manages the cyber security related procurement while they procure according to the law of public procurement (IP2:62).

When asked about security standards that were followed concerning cyber security, IP3 deflected the question and answered that there probably were standards that were followed but that we would have to direct further enquiries to another department (IP3:19). Concerning the "place at the table" given to cyber security when it comes to planning a project, IP3 mentioned that it was part of the application to the commission for financial aid for the smart city initiative but once again mentioned other risks as more important. IP3 also highlighted (IP3:35) the fact that the individual projects did not include cyber security at a planning stage. When asked about a secure modus operandi IP3 expressed that they were heavily invested and focused upon quality assurance and the quality of the output and mentioned that they should have to effectivise their work. (IP3:35) IP3 noted that there were, sometimes, someone from the digital development department could be included or asked in separate projects but implied it happened rarely.

Interviewee 6 confirmed that the is no cyber security strategy in the organisation but a there exists a policy handling these issues (IP6:24). Furthermore, IP6 states that the policy is focused on digitalisation in general and not specific for smart city initiatives. Smart city initiatives affects the organisation's systems and is usually a collaboration between different actors such as university and companies and thus, a policy for these projects is needed (IP6:24). IP6 also describes that when the decision is made that a project will be carried out, they discuss the cyber security risks involved in the project (IP6:45). IP6 mentions that the cyber security discussion is carried out by the IT department in collaboration with the relevant department to the smart city initiative IP6:65.

Moreover, if the project is perceived as a high risk project, the cyber security discussion should already have been done (IP6:45). IP6 describes future digital health systems as a high risk project.

> *"So once we connect this data on health, there will be some, discussions I guess since this will be very complicated so. That should be interesting in concern to security as well."*
> (IP6:45)

4.2.2 Organisational alignment

Interviewee 2 did not acknowledge that there were any particular threats toward smart city initiatives and mentioned that he was unable to estimate the general threat level and deflected this to their security coordinator (IP2:7). IP2 highlighted the fact that there are, in these smart city projects, different phases and different responsible authorities which he regarded as one of the greatest challenges (IP2:19).When asked about the main responsible for cyber security, IP2 mentioned that the IT department in the city were the ones to talk to if a general overview or more information was needed (IP2:24). IP2 deflected to people with more knowledge and mentioned that the responsible employees with security did not need to involve them.

"We meet our IT department regularly, our sister unit, we meet up regularly but then, it's more of a question that they don't need to, the ones responsible for cyber security, don't need to involve us if you say it like that, really. I think there are others who know significantly more than I do." (IP2:28)

When prodded about the different departments and the different spheres of responsibility, he acknowledged that the municipality was heavily divided as an organisation, and, beyond that, that they were very dependent on external partners. *"Yes, that's the way it is. It's very, the municipality is heavily divided as an organisation and then beyond that we are very reliant on collaborations with external partners."* (IP2:68)

Interviewee 3 (IP3:31) mentioned that the IT-department which is responsible for cyber security is rarely directly involved in smart city projects, merely involved when deciding what platforms to use. IP3 continues and notes that they might be participating as observers or asked questions at times.

Interviewee 5 stated that cyber security is not a part of the interviewees work and is instead handled by the IT-department (IP5:19). The interviewee describes if an overarching cyber security exists it was probably the IT department interest and responsibility, (IP5:21) however, the communicators and information department may also be included (IP5:27). Overall IP5 has a trust in the IT departments security measure both with handling external actors and their own cyber security (IP5:25). In the initial phase of smart city initiatives, no member from the IT-department or knowledgeable within cyber security is included (IP5:29). Furthermore, IP5 mentions that they are not mature as a smart city and that emphasis on smart city projects and the cyber security involved will probably grow with time (IP5:29).

Interviewee 6 brought forth the security task force and that they have a set of written standards for their processes. IP6 did not recall them all by heart, however. (IP6:20) IP6 mentioned that there were a lot of people working with cyber security, but attributed that they did so when working with the digitisation of the city.

They were not dedicated cyber security personnel, but could be included in smart city projects (IP6:38) IP6 does note, however, that the departments are decentralised and that each department had their own digitalisation units with overall strategic decisions concerning digitalisation was laid upon the mayor's department.

4.2.3 Policies and training

Interviewee 4 mentioned that they had policies concerning cyber security but all the same was unsure about the effect of them or if they were good (IP4:29) IP4 recognised that there are people that do not follow their policies as they are a big organisation with 70 000 employees. He acknowledged that there are risks when not all employees follow policies and noted that the risks were *"not that great, but they were there, of course."*

When asked about cyber security training and policies, interviewee 5 was generally uncertain and said that it was possible that it existed in the organisation but was really informed. IP5 acknowledged that the overall level was not that high, nor was the awareness and noted it was hard to get employees to follow general guidelines of not opening spam mails and such (IP5:35).

Interviewee 6 described that there is an introduction for every new employee where the information security policy is included (IP6:51). In addition, there is a one hour course that describe how an employee should behave in the workplace. However, there seems to be a lack of continued education of the employees (IP6:51).

> *"...every time we hire a new person you have to watch security videos before you get started, so in the introduction of new employees, there is also a one hour course, in term of how to behave at the workplace. However, I have been here for some years, and there has not been any follow-up, so."*
> (IP6:51)

4.2.4 Summary – organisational

Three of the respondents describe that there was not any overarching strategy of cyber security in their cities. However, in two cases the IT-department manages the cyber security part of the procurement. One respondent described that in their smart city projects cyber security is not a part of the planning stage with the exception of a few rare instances. Two respondents describe that the risks related to cyber security is not perceived as high in these projects and therefore, there is no need to include it in every smart city project.

On questions regarding risk awareness, the general theme was that cyber security is handled by the IT-department and was not a part of the project leader's tasks. At the same time, one respondent described that no one of the IT-department or knowledgeable of cyber security is included in the start of smart city initiatives. Furthermore, when asked about the cyber security risks in smart cities most respondents recommended us to talk to someone from the IT-department.

Lastly, three respondents described that there exists policies regarding cyber security and information security, although, the quality and effectiveness of them were questioned. Two respondents described that it was hard to make every employee in a large organisation to comply with the policies. It was also acknowledged that, even though employees receives policy education when employed, there is a lack of follow-up.

4.3 Financial

Financial factors might be a reason as to why cyber security is not a prioritised focus area, with some variety in this category as well. Literature note there is a generally high cost of IT - both implementation and maintenance and provide a reason as to why securing these assets and tools might be an under prioritised focus area when compared to other business and economical risks. This part of the chapter highlights these issues when interviewing the participants of the study.

4.3.1 Cost issues

Interviewee 2 recognised that cost is a problem (IP2:45), but notes that all development work costs money and that it is a question that they need to evolve on. IP2 highlighted that this is one of the reasons as to why the city applied for collaborations, both nationally and internationally. IP2 noted that since municipalities and cities are tax funded there is a constant need for a scale and different needs are weighed against each other. IP2 mentioned that the focus has been skewed from cyber security (IP2:56) and believes that the focus could be more directed toward cyber security. IP2 experienced that the financing possibilities did not steer toward a higher grade of cyber security: *"It's a little bit of a question of definition, but the financing possibilities has not steered toward cyber security, so to speak."* (IP2:56)

Interviewee 3 mentioned that information security is included as a cost factor but is not a primary concern in this aspect. The emphasis is on other economical risks such as overdue date of delivery or other circumstances that could trigger exceeding costs of the project (IP3:25). IP3 further clarifies the other circumstances: *"In the case of these projects, we get EUR 25 million, that is, a quarter of a billion for the project, and then we need to ensure that the project goes smoothly and arrives so we get the funding as planned, so it's a just as big a financial risk as we do with such projects. It is very important with time management and get past any delays and so on." (IP3:42).*

4.3.2 Not in budget

Interviewee 2 stated that the ICT component of smart city initiatives is about a third of the total budget and that there is a consistent cyber security budget in each of these projects (IP2:56). Furthermore, IP2 describes that there could be more focus on cyber security but proclaims that primarily, focus is not on cyber security (IP2:56).

IP3 describes that estimating the percentage of the budget the involves cyber security is difficult, but reckons it is under 5% of the project budget (IP3:54).

Interviewee 4 claimed that cyber security is included as an obvious part of the ICT budget (IP4:31) but did not mention that there were any specific budget posts for cyber security. IP4 instead hinted toward that the cyber security that was in place was from the products and systems from the suppliers.

Interviewee 5 also alluded to cyber security as being “a part of” the regular work (IP5:39), but didn’t know if cyber security was left any room in the specific budgets (IP5:37).

Interviewee 6 could not answer if the cost has been a factor in the past that made the city disregard cyber security (IP6:57). IP6 mentioned that cyber security and the trust of the citizens were high on the agenda and considered that if cost was an issue that would lead to discarded cyber security that project would be ignored.

4.3.3 Summary – financial

The financial aspect was not really acknowledged as a problem in cyber security for the respondents. However, one respondent described that it is a problem and in order to reduce costs the city applied for collaborations, both nationally and internationally. One respondent described that information security is a cost factor and included in the budget, however, other economical risks are prioritised. With this in mind, one respondent described that if cost would lead to discarded cyber security the project would be ignored. Another respondent described that cyber security was a part of the budget but that the proclamations do not focus on cyber security.

4.4 Outsourcing

Outsourcing is the last of the category of factors that could affect the prioritisation of cyber security in smart cities according to the literature overview. Considering the amount of collaborations with external partners as suppliers or contractors, which builds the digital infrastructure, there is a need for a high degree cooperation and affinity between organisations. Different factors for lack of focus on cyber security could be a high degree of trust on the external parties where cyber security is left as an inherent feature in supplied devices, systems or services. The other factor could be that the contracts are exhaustive and specify and detail different forms of cyber security as a part of the contract.

4.4.1 Trust

Interviewee 2 responded positively to the question of whether or not they trusted their suppliers and contractors and mentioned that only when thing happen and risks are found that it comes into question (IP2:66). As of yet, IP2 had not found any reasons to mistrust the city’s suppliers or contractors. IP2 responded that there is still a degree of ignorance when it came to the handling of data - both externally and internally and noted that there was a work of changing this.

Interviewee 4 recognised that the organisation has a person in charge of information security, but that security that involves protection of the system from cyberattacks is probably provided by the vendor that sold the system (IP4:23). The cities expertise is not to prevent hacker attacks, we buy that service from the vendors or the suppliers of the systems (IP4:23).

Interviewee 5 acknowledged that they from the outset assume that information security from suppliers and contractors is good (IP5:43), which has in turn created problems. *"Yes, because, I think we assume that IT security is good, but it has been shown that in some contexts it hasn't been as good as we primarily thought. But then we have, in those contexts we have discovered this, we have steered it in the right direction."*(IP5:43).

4.4.2 Contracts

Interviewee 2 mentioned that there have been situations in Germany in smart cities that there have been issues regarding who was ultimately responsible for cyber security and regarded the general discussion around open data as 'naive' (IP2:15). IP2 highlighted that the fact that the naivety created situations where the issues of cyber security were put on external parties, big IT firms, which did not have the same interest as cities and municipalities (IP2:17). IP2 explained that this created greater issues in cities not being able to deliver the expected results, which created a higher drive in increasing rules and best practices in EU initiatives. IP2 noted that this discussion had not yet reached Sweden, however, and that the same problems were found in IP2's city. *"The municipality has not stepped up and taken responsibility and told what everyone were going to do, which then lead to that you were sometimes in the hands of big IT-firms. This has happened in Germany, for example. This has then lead to the fact that you have not been able to deliver the proper results, which then lead to them being in negotiation with a data provider who do not have the same interests, that is, the interest of the public. They were very clear with that this has to be tightened, that discussion has not yet been here but in parts of our system we also have that problem."* (IP2:17) IP2 recognised there were still contracts that were not in line with the organisation's policies and that the knowledge of where data was stored was relatively uncertain. As a cure, IP2 suggested better procurement contracts. (IP2:66)

Interviewee 4 described that cyber security is a natural part of the budget as well as the procurement although it is not explicitly listed (IP4:31). IP4 describes that depending on the project the the risks involved the emphasis on cyber security in the contracts vary (IP4:31). IP4 also describes that cyber security is an incorporated in how the organisation works: "*So, we spend money on cyber security - it is involved in everything we work with."* (IP4:31)

When asked about the trust put in external parties, interviewee 6 mentioned that it is a very important criteria and that they had to live up to certain standards to be able to deliver products or services to the city.

4.5 Other inputs

Other inputs denote interesting points and especially themes that were not found in the literature but were likewise themes that could explain or give insight into why cyber security is not a prioritised focus area for smart cities.

4.5.1 External directives

Both Interviewee 2 (IP2:13, 17, 33) and Interviewee 3 (IP3:42, 62, 64) mentioned external demands from external financiers such as the European Union. This formed a basis for much of the work that was done in a smart city context and there was a focus toward functionality and the deliverable in these projects instead of a safe, stable and secure foundation for further smart city initiatives. IP2 experienced that there was a general naivety in the commission for smart cities in the European Union and that there were improvement areas when it came to open data (IP2:15, 17). IP2 also mentioned that the risk analyses that were done on projects with directives from the EU were based on an outline provided by the European Union. IP2 mentioned that many of these questions are also set by the state as well as the EU as these projects were financed and driven by the external financing. (IP2:32) The sponsors set the agenda and cyber security was added on by the city as part of their daily work. A noteworthy quote was from IP3 which was previously mentioned in 4.3.1:

> "*Not more than what I have described earlier. That information security is a part of it, but there are many other risks that we consider are bigger and more comprising. In projects like these, we receive 25 million euros, that is to say quarter of a billion for the project and then it's the matter of making sure that the project goes smoothly and reaches the end, so we get the financing that was considered, so it's a big economical risk that we handle in projects like these. It's very important to handle time plans and get past potential delays and so on."*(IP3:42)

Interviewee 3 states that the financing they receive is given and that the city will have to make sure that it runs smoothly (IP3:42). IP3 points toward and argues that they have to be able to make sure that they receive their financing, which they consider as their main risk. When asked about functionality above anything else, IP3 agrees and notes that functionality is top priority. Also mentioned by IP3 is that demands set by external financiers (IP3:62) are in a contractual attachment and that the risks in these demands and that the city see are not prioritised, instead there are a great deal of other risks which are given more space (IP3:64)

4.5.2 Maturity of smart cities

The last common theme of the empirical data involved the smart city maturity. IP4 stated that the strategy for becoming a smart and online city was taken in April and started implementing smart city initiatives in November (IP4:4). Therefore, IP4 described that they are considering new projects, but it only exists in a small scale right now (IP4:4). IP4 also claimed that they were not often exposed to cyber threats (IP4:35) and used this as a reason when asked if IP4 experienced that enough money was spent on cyber security.

When asked about the involvement and closeness of the IT department in smart initiatives, Interviewee 5 stated that they were not that close (IP5:29). He argued that this is because the city had not come far regarding smart initiatives. He noted that the drive for further connectedness and 'smart' are on their way but stated that in IP5's experience there was no real progress so far.

4.5.3 Previous incidents

Another interesting theme this paper identified was that cities that have experienced incidents prior were more aware of the risks and had more comprehensive cyber security measures. IP4 described that cyber security was very important for the city because of the high amount of attacks all the time (IP4:25). IP6 mentioned that a security breach in their system lead to changed cyber security policies as well as more attention to smart city projects and cyber security (IP6:53). IP6 further describes that: *"...hackers accessed our open data portal and in 2014 we actually had an accident where some data was leaked which was personal. And after that we sat down and, security task force in the city that runs through every smart city initiative and has certain criteria that has to be fulfilled. So that's a lot of attention to that."* (IP6:2). IP4 further mentioned that it is generally easier to prioritise cyber security in larger cities (IP4:25).

5 Discussion

This section of the paper will go through an in-depth analytical discussion regarding the empirical findings in relation to prior research. This part will also strive to elucidate the thoughts and prioritisation of decision makers in smart city projects in regards to cyber security. The chapter is divided into the same categories as found in earlier chapters in an endeavour for higher pedagogy.

5.1 Knowledge and awareness

As smart cities evolve, new technological innovative solutions create additional security threats and challenges (Chourabi et al., 2012; Elmaghraby and Losavio, 2014). Chourabi et al. (2012) outlines high cost of security applications, accessibility, privacy of data, viruses, worms, threats from hackers and trojans as some of the challenges from smart cities. These need to be considered when building smart cities since it includes building the foundation for future systems (Heo et al., 2014). In order to improve the quality of life for its citizens the cities requires the highest level of security (Bartoli et al., 2011) because it is only a matter of time before the digital foundation of smart cities will fail (Townsend 2013). Thus, smart cities require a proactive cyber security while Johnston and Hale (2009) describe that organisations tend to utilize reactive cyber security approaches.

5.1.1 Risk awareness

McFadzean, Ezingeard and Birchall (2007) describe that a common reason for lack of emphasis on cyber security is dependent on the top managers perception of the risk. Therefore, the respondents’ perception of present and future risks of smart cities could be of interest in order to explain contributing factors for the lack of cyber security focus. In the empirical findings, three respondents acknowledged that the future holds threats for smart cities but in the present state there exists no real threats. Thus, the perceptions of the present risks are generally rather low, which could explain why cyber security is not prioritised. Although the present threat may not be considered as a high priority, smart city initiatives require to account for the future systems that will be built or communicate with the implemented systems which this papers empirical findings did not recognize. Therefore, the respondents’ statements contradict the proactive approach of building a safe foundation, which Heo et al. (2014) and Bartoli et al. (2011) suggest. Furthermore, IP3 described that there is no comprehensive difference between pre- and post-smart city initiatives; the only real difference is the amount of data. Furthermore, the respondents did not seem to acknowledge the fact that they are building the foundation of smart city that Heo et al. (2014) and Bartoli et al. (2011) describe but rather consider smart city initiatives as any other city project. Thus, the respondents did not seem to view the smart city initiatives as a comprehensive change of the city, which could explain the lack of the long-term perspective.

From the outlined risks of smart cities, the respondents only really focused on the privacy issues with smart cities and not the high cost of security applications and threats from hackers, viruses, worms and trojans outlined by Chourabi et al. (2012). These interviews were carried out at the same time as an EU regulation regarding data protection and privacy, which could potentially skew the considerations. However, if these risks are not addressed there is a high probability for undefended smart cities, something which Khatoun and Zeadally (2016) describe as high value targets for cyber attacks. Smart cities need to test their cyber security, devices, features and encryptions in order to become resilient to cyber attacks (Khatoun and Zeadally, 2016).

5.1.2 Knowledge

A smart city should improve the life quality of its citizen's though innovative solutions (Heo et al., 2014) while also building a robust digital foundation for future implementations where cyber security is prioritized from the start (Bartoli et al., 2011). This requires knowledge and a holistic long-term perspective from the project leaders. However, a proactive thinking about cyber security is not mirrored in the empirical results. Instead one of the respondents did not acknowledge any cyber security flaws or risks in smart cities and the rest of the respondents had a general knowledge of privacy issues with possible information leaks rather than securing the systems. As described by Johnston and Hale (2009) too many organisations tend to utilize a reactive approach to cyber security planning which in turn helps moulding the buggy and brittle smart cities that Townsend (2013) and Kitchin (2014) describe. Since the respondents seemed to lack a long-term perspective, chances are that the respondents would build smart cities that are reactive instead of proactive. Thus, lacking knowledge, which includes long-term perspective of smart city development, could be identified as a contributing factor for the lack of focus on cyber security.

5.1.3 Non-challenge

According to Singh et al. (2013) cyber security risks need to be identified, compared and rated in order to efficiently approach the array of different risks specifically. Chabinsky (2010) also suggests risks analysis in order to break down cyber security issues in to the smaller components.

However, the majority of the respondents described that cyber security is not a major issue for their organisation. Instead, they alluded to other more prioritised issues that have more direct effect on the smart city projects. According to one respondent the risk analysis is grounded on the requirements of the EU-commission and apart from this risk analysis featured no further specific cyber security risk analysis. The EU-commission is described as the financier of the smart city initiatives in the respondent's city and if the demanded risk analysis from the EU-commission does not acknowledge issues with cyber security, additional cyber security analysis was probably not conducted.

Furthermore, it is hard to catch hold of more specific details about the risk analysis conducted in the respondents' organisations, thus, it is hard to discuss whether the cities risk analysis involved identifying, comparing and rating cyber security risks as Singh et al. (2013) and Chabinsky (2010) prescribes. However, cyber security was not perceived as a major issue or challenge in the respondents' organisations risk analysis.

5.2 Organisational

From the theoretical model that the literature overview gave, it is suggested that in order for an organisation to reach a favourable level of cyber security, it needs to be considered as an overall business matter (Goles, White and Dietrich, 2005; Johnston and Hale, 2009; Kwon et al., 2012; Chabinsky, 2010; Wang, Ali and Kelly, 2015). This is highly related to strategic alignment between business and information technology strategy. The informants generally had issues naming a specific cyber security measure, which lends support to the assumption that, the cities and municipalities did not have pervasive governance of cyber or information security. By not having an Information Security Governance (ISG), according to Johnston and Hale (2009), it has an adverse effect upon the alignment of business and IT risk management. This is something that Kayworth and Whitten (2010) argue is negative for effective cyber security in an organisation, obviously. Also important to consider, as pointed out by Doherty, Anastasakis and Fulford (2009) and Puhakainen and Siponen (2010), is the compliance of employees throughout an organisation. Kayworth and Whitten (2010) conclude in their study that effective cyber security is applied by pervasive organisational and social alignment mechanisms together with an overall competence in technology and a socio-technical focus on cyber security. By creating a security culture in an organisation, compliance comes naturally and will likely be a prioritised matter.

5.2.1 Business alignment

Three of the informants mentioned that they had no overarching cyber security strategy and the informants were in most cases deflective when trying to explain the cyber security strategies or guidelines. IP3 directly voiced that cyber security was seldom included at a planning stage in individual projects, merely at procurement and application stage. This is intriguing considering the recommendations by many, notably by Bulgurcu, Cavusoglu and Benbasat (2010) and Wang, Ali and Kelly (2015) who state clearly that cyber security needs to be involved not only in the technological sphere, but also in softer values such as in security policies, human factors, third-party chains, insider threats and more. A correlation could be drawn to the argument of McFadzean, Ezingeard and Birchall (2007) who claims that the lack of focus on information security stems from top-level management perception of cyber security risk. Nothing was mentioned by our informants regarding meetings with top-level management about cyber security.

The focus in smart city projects, experienced from interviewing our participants, was often on the functionality; the business goals and the deliverable. It seemed cyber security was often overlooked because of this. This is something that is bound to happen when cyber security is not considered as an overall business risk or aligned into the overall strategy (Goles, White and Dietrich, 2005; Singh et al., 2013). Johnston and Hale (2009) strongly recommend aligning core business goals, processes and assets with cyber security as a complete enterprise governance process when considering cyber security in an organisation.

As mentioned by some of the respondents (IP4, IP5), they often alluded some cyber security issues to the phenomenon of a ‘big organisation’ which is interesting, considering the findings of Knapp et al. (2006) that big organisations had less issues when it came to top management support regarding cyber security when the organisation had more than 10.000 employees. They do, however, claim that top management support is the main issue in most cases, which is interesting as there were few mentions of top management, merely in cases when directives came from a higher instance like the state or the EU.

Von Solms and Von Solms' (2005) thoughts apropos information security and that it needs to be a board level responsibility and the argument that cyber security should instead be named 'business security' is poignant during this part of the discussion. This is because the informants in the study conducted demonstrated there is a clear divide between business goals and ensuring the security and safety of these projects in regards to cyber security risks.

The respondents often expressed (IP2, IP3, IP6), as previously mentioned in the knowledge and awareness section, that there were other aims or focuses that were more important. Johnston and Hale (2009) attribute in their study that a disparate in perspectives between ISG implementers and non-implementers has multiple sources. They name top management, a supportive organisational culture and a general awareness and responsibility by employees. Employees need to have a higher grade of training in cyber security, then, in order to achieve a higher awareness. We believe that high integrated work processes between different departments and employees in smart city projects is to prefer to establish a higher, general cyber security level. This is something that, as of yet, seems to be hard to enact, which we will discuss further in the next section.

5.2.2 Organisational alignment

There was an overall distance from the decision makers in these projects and cyber security and instead reliance upon personnel or departments 'tasked with' cyber security instead. This, however, creates a problem due to the fact of a high decentralisation and segregation in the organisation between the different departments, which all of the respondents answered or hinted toward. Kayworth and Whitten (2010) argue that in order to achieve a decent degree of cyber security an organisation has to have employees with an overall competency in technology and measures of organisational and social alignment mechanisms in regards to cyber security. This is also an argument by Singh et al. (2013) who mention that technology is absolutely a part of the solution, but one that is only accomplished together with organisational and human measures and actions. By the empirical data found, there seems to be an insufficiency of these organisational and human measures in smart cities.

Noteworthy was that IP2 mentioned the problem of there being different phases with different responsible authorities as one of the top challenges to overcome in regards to smart city projects. IP2 and IP3 claim that the IT departments and personnel tasked with cyber security are rarely involved directly in projects. IP5 specifically mentioned that no members of the IT-department or tasked with cyber security were involved in a planning stage.
Respondents often pivoted when asked about slightly technological matters, which also lends credence toward an assumption regarding fractured organisations with few collaborations and inter-departmental training and a low organisational alignment.

Something also worth noting is the problem of having enough competent IT employees in a public-sector organisation, according to Alawadhi et al. (2012) thoughts about the non-attractive workplace for young IT professionals. If this is the case, it might be an issue finding the right talents needed for the work required in regards to information technology and cyber security.

5.2.3 Organisational policies and training

Cyber security policies aid organisations to create awareness and compliance of cyber security regulations since cyber security is not a technological issue (Chang and Lin, 2007; Bulgurcu, Cavusoglu and Benbasat, 2010). Generally, the respondents answered that there were no pervasive cyber security training or policies. There was a lack of follow-up and the effectiveness was in doubt when asked about them. As Siponen, Mahmood and Pahnila (2009) claim, the visibility of the policies and training has heavy implications on the employee’s behaviour for policy compliance. This has plausible effects on the level of cyber security in smart city projects. However, cyber security and policies is closely related with the top management’s perception of cyber security and could be the reason as to why there are no policies or training.

5.3 Financial

As has been noted in 2.4.3, financial factors were seen as having a critical role in smart city initiatives. Pierce and Andersson (2017) highlight the issues of conducting cost-benefit analyses in general with smart city projects also contended by Alawadhi et al. (2012). It comes as no surprise then, when combined with the high costs of IT - personnel, implementations and maintenance - (Chourabi et al., 2012; Sommestad, Ekstedt and Holm, 2013) as well as high cost of cyber security (Gordon et al., 2005; Rowe and Gallagher, 2006) and a general lack of alignment between business and security needs (Kayworth and Whitten, 2010), financial factors has a potential in greatly influencing the lack of prioritisation on cyber security.

5.3.1 Cost issue

However, interesting to note is that none of the respondents cited a financial factor as being crucial in the decision regarding cyber security implementation in spite of what has been established by previous research. Even though IP2 recognised the problem with cost of cyber security and IT, it was merely one of many development costs and that the focus is skewed from cyber security. During these answers, no thought was given to the cost of breaches, which has a potential to become tremendously costly for organisations (Campbell et al., 2003; Rowe and Gallagher, 2006; Kannan, Rees and Sridhar, 2007; Alawadhi et al., 2012, Kuypers, Maillart and Paté-Cornell, 2016). Even though the tenuous effect on stock prices has no real importance to public sector organisations, reputation damage could have potential serious consequences in a public-sector organisation.

Instead of cost as a factor for disregarding cyber security, other challenges were cited as being more important and economical risk was often alluded to by IP3 and used an example when external financing was given the economical risk was highly prioritised. IP6 also stated that functionality; the 'present problems' were of higher priority - namely, the functionality of the projects. IP2 specifically mentions that the "financing possibilities" had not steered toward cyber security, which is an interesting point to consider. The role of the financiers will be discussed below, in 5.5.1, in further detail. Also worth mentioning is the argument highlighted by Alawadhi et al. (2012) that multiple city governments has not garnered enough financial support and thereby lost key employees working with IT as well as missing opportunities of upgrading and updating critical systems for smart cities. Also noting the financial support is the thoughts of Soomro, Shah and Ahmed (2016) who specifically note that the financial provision is one of the top deciding factors whether cyber security succeeds or not.

5.3.2 Not in budget

Gordon et al. (2005) argue that there are inherent issues with budgeting for cyber security which could create the tendency of there being problems with aligning business goals and cyber security in budgets, which Kayworth and Whitten (2010) claim. None of the respondents had any specific details about the budget for cyber security, and most assumed (IP2, IP3, IP4, IP5) it to be an inherent part of the IT/ICT budget with no additional, overarching posts.

Making an assumption, by not having an overarching strategy for cyber security it has consequences on the space left for cyber security when discussing budgets, which then affects the amount of awareness of it in the organisation. There seems to be a negative spiral affecting the focus on cyber security in smart city projects.

5.4 Outsourcing

Outsourcing is the last of the category identified in the literature review, which possibly affects the focus on cyber security in smart cities. Smart cities initiatives are involved with collaboration between different external partners such as suppliers or contractors in order to build the digital infrastructure. Identified factors for lack of focus on cyber security includes that cities could have a high degree of trust on the external parties and their ability to secure the products or services. Another possible factor could be that the contracts specific in detail different cyber security clauses in the contracts and therefore, have outsourced cyber security to external partners.

5.4.1 Trust

Cyber security is a complex field and only a few organisations have the adequate resources or motivation to fully handle the cyber security defence within the organisation (Gonzalez, 2005). Hence, it has become necessary for organisations to outsource cyber security processes and trust that vendors utilize appropriate measures. Three of the respondents described that their organisations trust their vendors to provide sufficient cyber security in their smart cities. One respondent described that cities' expertise is not to prevent hackers and thus these services need to be bought from external actors. The respondents did not find any reason to mistrust the cities vendors. However, one respondent mentioned that sometimes the cyber security of their providers was not as good as they primarily thought, and in these cases where cyber security issues have been discovered they were remediated. However, it seems problematic that the organisations with limited cyber security knowledge need to evaluate their own system in order to find cyber security issues.

5.4.2 Contracts

Khalfan (2004) states that when an organisation decides to outsource cyber security defences the service provider should be thoroughly evaluated since security breaches could seriously harm the business. Furthermore, specific cyber security contracts should be signed in order to overcome vulnerabilities of the systems (Khalfan, 2004; Wenge et al., 2014). The contracts should involve robust arrangements for cyber security, particularly in the service-level agreement. One respondent describes that cyber security is a natural part of the budget as well as in the procurement. However, cyber security is not explicitly listed, although if cyber security is perceived as a high risk, the contracts could vary. Thus, cyber security seems to be something that some of the respondents include in their contracts, to some degree. However, Carr (2016) describe that the private sector is not willing to be held accountable or responsible for national security breaches, which further aggravates the problem. One respondent describes an example of how big IT firms; cities and municipalities have different interest. Therefore, better procurement contracts are needed.

5.5 Other inputs

Other inputs were left in order to analyse other themes that have not been included in previous literature. Common themes among the answers by the respondents were insinuations toward financiers’ directives and their demands, which affected the prioritisation in smart city projects that were directly financed from external actors. Another strong theme found was the deflection on the maturity of the smart city status in the respondents’ cities when it came to the amount of cyber security in place. Also found was that previous experiences set a strong precedent in regards to cyber security.

5.5.1 *Financiers’ directives*

As Ferrer et al. (2013) mentions, funding is expectedly of great importance in order to succeed in smart city projects. Ferrer et al. do, however, mention that smart city investments are of a high-risk level due to long expected profitability time and the large amount of money required. One can then assume that the focus will therefore be on being able to actually implement the smart city project, i.e. the functionality of it and ensure full funding. It’s also probable that focus is shifted toward the demand from financiers who might not in first stage be interested in investing in cyber security, in line with what IP2 notes.
Specifically, what IP2 had experienced before when the city of Umeå had been chosen for pilot projects, cyber security was not of concern by the financiers and instead that the focus was on building the platform - on the deliverable.

This was also agreed with by IP6 who claimed that the problems were on the present and what they could solve at the moment. IP3 also hinted toward a bigger pressure from financiers on following through with investments in smart city projects and that the main priority was on the deliverable and that functionality would be implemented the way the financiers wanted. This in order to "ensure the financing" that was promised, noticeable in the quote used in 4.5.1. As Baccarne, Mechant and Schuurman (2014) states, both national and transnational governments continue to support and provide funding for smart cities and are therefore key actors in the decisions taken in smart city projects they set the tone and prioritisation. As IP2 mentions, cyber security has not been a main issue and merely been glanced over and has therefore been left on the agenda for the local governments.

5.5.2 Maturity of smart cities

An intriguing thought regarding the current threats toward smart cities is spoken by one of the informants is the following:

> *"In reality, there is no difference now in regards to earlier, it's just that we are gathering more data now because it's easier to collect it and also easier to put in controls. There are both problems and possibilities."* (IP3:17)

This is most probably a shared thought of many in higher levels of management and could be an explanation for many of the issues faced by smart cities. An unwillingness of adaptability when faced with new problems is a dangerous mind-set, especially when considering the dangerous possibilities when cities' critical infrastructure is connected and possible to remotely attacked.

"Far too many firms take a reactive approach to information security planning" Johnston and Hale (2009) claim that organisations that have a proactive approach to security planning are rare and that the proactive approach is the most common, which they claim is a critical problem. Connected with the empirical findings, this is something that rings true in most cities. Heo et al. (2014) argue that the infrastructure and systems that are being built and implemented need to be done so with expandability considered and integrated for interoperability, which also lends itself as true for cyber security. In essence, they have to be built with extensive planning for future iterations, which is not the case, found in this study.

The fact that there are so many projects and initiatives afloat already and the overall focus on cyber security has been relatively low is intriguing considering Bulgurcu, Cavusoglu and Benbasat (2010) and Wang, Ali and Kelly (2015) thoughts that cyber security will never be as efficient when implemented at an early implementation stage. A parallel can be drawn to previous literature's (Igure, Laughter and Williams, 2006; Munro, 2008; Gold, 2009; Bradbury, 2012; Syed et al., 2017; Thibodeaux, 2017) assertions of the unsecure connected SCADA systems. Infrastructure, then, is being implemented with a generally low cyber security plan or strategy in mind, which has a high risk of producing flaws further down the road. Kuilboer and Ashrafi (2016) and Syed et al. (2017) all emphasize that cyber security is something that needs to be included at a planning stage of a product, system, project - anything that is connected - in order to protect the products and systems, and thereby, then, information, business and human lives.

Even though the smart city projects might not have reached a mature stage in some cities, it is imperative that cyber security is something that is considered at an early stage of the initiatives. All the respondents considered the projects by themselves and had no overall and pervasive cyber security strategy or process that tied different projects together. The lack of a complete and general risk awareness in chapter 5.1.1 regarding cyber security could be the cause of this as a complete picture of what is going to happen down the line, in the future, is needed in order to close the cyber security risk hatches. This is mirrored in IP2's thoughts about a current naivety regarding the role of the municipalities and city governments in smart city projects in the EU-commission for smart cities. This in turn has far reaching effects on smart cities in Europe, presumably highly on funding from the European Union.

5.5.3 Previous incidents

Also worth noting is the thoughts expressed by IP6 where it was mentioned that there had been a previous cyber security incident in the city which shifted attention to the issue. This was something that also IP4 claimed, that the priority on cyber security was because of the previous incidents and threats. The theme seems obvious, of course, that prior experiences sets a general precedent and if incidents have happened organisations are by necessity generally more mature in regards to cyber security. However, as mentioned in previous paragraphs, it's vital that cyber security be planned from the start in a proactive manner.

6 Conclusion

The ambition of this study was to identify and understand the reasons for the lack of focus on cyber security in smart cities. The following part of this paper will summarize the research findings in order to answer the research question.

What are the reasons for the lack of focus on cyber security in smart city projects?

A lack of cyber security in smart cities has dire implications. The consequences from breaches range from mortal danger to large economical losses. The literature rarely looks into the combination of smart city phenomena and cyber security and has failed to reach a conclusive paradigm regarding these two concepts.

Through our empirical findings the research paper found that possible reasons for the lack of focus on cyber security is that there is a generally low level of strategic alignment within the respondents' organisations. Information systems strategy seems to be underrepresented in the organisations, which has implications for further work with information technology and systems. Furthermore, organisational strategy is not aligned with IS strategy and the organisations were segregated; the departments were fully independent and merely had brief dialogues. The top management's perception of cyber risks was also generally quite low as there were no proper agenda for cyber security in the organisations, according to the respondents. Cyber security was not considered a board level responsibility nor included as a business risk. There were no proper or pervasive cyber security policies or training. Directives to the projects leaders were to mainly focus on pure business risks instead. Also found was that in smart city projects, experienced from interviewing our participants, focus was shifted toward the functionality, i.e. the business goals and the deliverables because the cyber security risks were considered as insignificant in comparison. Responsibility for cyber security defence is solely distributed to the IT-department due to segregated organisations and a misalignment between information systems strategy and organisational strategy. Moreover, the respondents' organisations found no reason to mistrust their suppliers/contractors and some level of cyber security is often included in the procurement contracts.

In addition, we found that financial factors did not have a direct effect on the lack of focus on cyber security, and instead indirect effects in the form of prioritising ensuring enough funding in the form of a deliverable focus. A possible a reason for this could be the immaturity of cyber security perception as a whole, whereby cyber security is not acknowledged as a risk nor a substantial post in budgets.

Infrastructure that is now being implemented will serve as the foundation of all cities in the future, which creates an exigent need for long running strategies in order to secure information, businesses and protect human lives. As of now, cyber security in smart cities may seem of concern to only a small group of practitioners, however, as smart cities evolve and expand it should in fact concern anyone who lives in a smart urban area.

The expected contribution to the IS field of study is to explore the reason why there is a lack of focus on cyber security within the smart city context, especially when security is a constant issue in other IS fields. This research paper outlines a complex web of reasons for lacking cyber security in smart cities that affect each other. However, the reasons found for lack of focus on cyber security in smart cities generally resemble previous literatures factors for lack of cyber security, and thus, is not a unique context.

Although we grant that there exists an inherent issue deciding what level of cyber security is enough, we still maintain from our research that the current level of focus leaves much to be desired when considering the oncoming challenges.

6.1 Limitation

The scope for the research was limited in regard to participants involved, mainly due to the qualitative research approach. However, the selection was random and included four different cities in Scandinavia. Also required is the reflection upon the political climate Scandinavian cities and the requirement of general security in comparison to other countries, which could potentially be more, exposed to foreign powers and malicious actors. Other countries could possibly have stricter regulations and demands on the security aspect.

Another thing worth noting is the size of the cities. The case cities inhabitants span from 100.000 to 950.000 inhabitants and thus does not include the higher or lower populated cities. However, the paper’s emphasis is on identifying the reasons for the lack of focus on cyber security, while future research could illuminate the relation between differently sized cities and further reasons.

6.2 Future research

The study identified three different areas for future research. Firstly, the study found that financier’s directives has major implications on the prioritisation in smart city projects. The study also identified there was some level of naivety in regard to cyber security according to the respondents. The overarching leadership and responsibility of cyber security has previously been mismanaged in other EU sponsored smart city projects, which has led to an overall confusion and lack of cyber security. Future research could potentially explore the previous examples of EU directives on smart cities and offer explanations and offer practical implications for European Union sponsored smart city projects.

Secondly, smart city maturity and the deflection of responsibility was often experienced in the interviews and denotes that an overall picture of the situation is lacking. The obvious explanation is that most of the cities interviewed do not have comprehensive experience of smart city projects and thus need time to mature in order to close the cyber security risk hatches.

Lastly, the empirical findings implied that cities that previously had experienced cyber security incidents generally had more awareness and mature in regard to cyber security. However, our study could not draw any conclusions and future research could explore how cyber security breaches in smart cities affect taken cyber security measures

Appendix 1 – Interview 2

Sex: Male

Age: 40 +

Alias: A

Date and Time: 2018-05-03, 08:01

Type of interview: Skype interview

Duration: 48:58

A: Interviewee

G: Gustav Jansäter

J: Joel Olsson

#	Speaker		Code
1	G	Då kommer en lite generell fråga här att börja med. Och det är, upplever du att det finns ett tillräckligt fokus och tillräckliga aktioner tagna, för cybersäkerhet eller informationssäkerhet? Vi använder dessa begreppen rätt analogt, alltså cybersäkerhet och informationssäkerhet.	
2	A	Ja precis. Nej det gör det ju inte. Vi har flera som, vårt IT kontor, jag jobbar ju ganska aktivt med dem här frågorna, så att. När vi sätter ihop smarta städer projekt så är det alltid en del av det, men absolut behöver det. Frågorna är ju ständigt aktuella,	K&A-RA
3	G	Vi har sett lite, att det blir lite mindre fokus på just cybersäkerhet i smarta initiativ när vi har kollat rundor, och det är det som är bakgrunden till vår studie.	
4	J	Men om vi fortsätter då, vilka risker ser du med smarta städer initiativ?	

5	A	Det finns flera risker, men om man kopplar det mot, man kan säga såhär att smarta städer, vi har ingen egen, detta är ju en definition som andra lägger på oss, och det finns ganska mycket finansiering kopplat till smart städer, exempelvis inom EU. Och då är ju smarta städer att koppla ihop ICT infrastruktur med transport, energi, bostadsbyggande. Så det är ju den rollen som jag har haft och det som, det som har varit väldigt tydligt från EU hållet är balansen mellan den offentliga och privata kontrollen av data. Det som kallas för öppen data, där har man ju varit väldigt tydlig med att det är kommunen eller det offentliga som ska ha kontrollen över ägandet av data och dela med sig, mycket vinsten med smarta initiativ ligger i det. Vi har också ett nationellt projekt kring IoT tjänster fastighetstjänster, som genom Vinova. IoT Sweden program där den frågan är rätt aktuell, och det kämpar vi ganska rätt mycket med, den balansen. Vi lyckas i vissa fall och ibland inte, det är mycket upphandlingar och mycket olika dataset som ligger hos många olika aktörer som ska samordnas, jag skulle inte säga att vi är i land med detta, men det är en stor utmaning som vi har utifrån de kraven som ställs. Sen när det gäller cybersäkerhet så är jag inte riktigt personen som kan uttala mig om exakt vilka risker som finns relativt det. Men utmaningen, det är något som vi har prioriterat väldigt mycket, hur vi får kontroll på strategisk data, och vi har också kommunala bolag som är en gråzonsaktör som lyder under offentlighetsprincipen, och stora dataflöden, energibolag med flera. De arbetar mycket med att optimera sina processer och erbjuda tjänster till sina kunder och invånarna i staden.	OI K&A-RA
6	G	Känner du att det finns en hotbild mot de smarta projekten i staden?	
7	A	Nä, inte mer än alltså, det finns, jag kan inte bedöma den generella hotbilden, den är jag inte ansvarig för så den, vår säkerhetssamordnare har hand om den. Men det finns inget särskilt, utan detta är en del av vårt vardagliga arbete med verksamhetsutveckling, det är ingen generell hotbild om de.	O-OA K&A-RA
8	G	När ni har smart city projekt, har ni någon säkerhetsstandard som ni använder vid införande?	
9	A	Problemet är väl att det finns rätt många säkerhetsstandards, nu har vi ju rätt många system och tanken är att vi knyter ihop många olika aktörer men vårt stora lighthouse projekt som heter Ruggedised, där är vi 7	

		olika aktörer bara i Umeå, dessutom har vi andra städer runt om i Europa. Oftast så är det olika fastighetsägare och olika system, utan att vara expert på det här området, så hur det kan kopplas upp mot den rollen som vi har då, som förvaltare av data och såhär, där har vi ett åtagande gentemot EU-kommissionen. Vi är eniga om att vi ska ge möjligheterna men vi har inte hittat exakt hur det ska gå till. Jag tror det är många städer som kämpar med den där utmaningen, vissa har privatiserat detta och då har tappat kontrollen över sin data och då får man börja betala för det och ja, och vi har delvis de problemen.	
10	G	Intressant, i Umeå kommun, har ni en övergripande cybersäkerhetsstrategi?	
11	A	Vi har en IT-strategi men vet inte om detta ingår, jag skulle vilja hänvisa det, den frågan kan ni få ett snabbt svar av en kollega. Vissa av dessa frågorna är av den karaktären att jag helt enkelt inte vet.	K&A O-BA
12	J	Finns det någon av riskanalys när ni inför ett nytt smart city projekt.	
13	A	Det är två olika frågor egentligen, i alla typer av projekt så genomför vi någon typ av riskanalys. Då tittar man på saker som, hur passar detta in i den långsiktiga planen för staden och så här. Det är en typ av riskanalys, det är det som är lite lurigt med smart city projects, för det är enorma stadsbyggnadsprojekt, och är därför av en annan karaktär än cybersäkerhet delen av det. Så att, det är väldigt bra frågor. Den riskanalysen som vi har gjort inom smart city projekt, tror jag inte har, där baseras det väldigt mycket på de frågor som kommissionen har ställt, snarare än att vi har gjort någon tydligt cybersäkerhetsanalys. Så den interna som vi möter upp för att gå in i den här typen av satsningar följer ordinarie strukturer. Så vi ger ingen särskild riskanalys för ett smart city projekt. Och om man ska vara helt ärlig, så är ett smart city projekt i stor utsträckning som vårt ordinarie arbete, så det är ingen skillnad. Vi ser oss som en smart stad, med våra styrkor och svagheter som vi har i det ordinarie. Så fungerar det ordinarie arbetet i kommunen, att man gör analys när man går in i nya satsningar, och då kan det handla om personal, nyckelpersoner, ja, tillgänglighet och sådär men exakt hur det ser ut kring cybersäkerhet, jag är inte inne i de detaljerna i frågor, så jag kan inte svara på det faktiskt.	OI K&A-RA

14	G	Men det är väldigt intressant det som du nämner, att det kommer från högre instanser både nationellt och internationellt i form av EU. Och att det inte riktigt finns några riktlinjer kring cybersäkerhet i dessa projekten.	
15	A	Min bild, jag har varit mer involverad kring diskussioner kring öppen data, och där har jag upplevt att det finns någon typ av naivitet för några år sen.	
16	J	På vilket sätt är dom naiva?	
17	A	Jag vet till exempel vi hade besök av EU-kommissionären för smart städer för några månader sen, då pratade hans rådgivare just om det här att, många av deras lighthouse städer i EU, har haft problem med. Kommunen har inte tagit på sig ledartröjan och berättat vad man ska göra, så då har man ibland hamnat i händerna på stora IT-firmor. Det har hänt i Tyskland bland annat. Och då har man inte kunnat leverera de resultaten sen, att man hamnar i en förhandlingssituation med en dataleverantör som inte har samma intressen, alltså allmänhetens intressen. De var väldigt tydliga med att detta skulle skärpas till, den diskussionen har inte varit hos oss, men i delar av vårt system så har vi också det problemet. Vi har enskilda datasystem som ligger i den privata sfären.	OS-C OI
18	G	Och det är lite som det problemet innan, att det finns så många olika aktörer och ansvarsområdena kanske inte är uppdelade på ett tydligt sätt.	
19	A	Ja, och att det kommer vid olika faser, det är olika upphandlingar vid olika faser och det är olika huvudmän och så. Den samordningen är kanske det som vi ser som den stora utmaningen, eller så som jag och mina kollegor är inblandade väldigt mycket i att se hur vi kan få detta att samverka för att skapa samhällsnytta.	O-OA
20	G	Det är lite i form, vid samma beröringspunkt som det här med många olika aktörer och liknande. Det är många olika saker som händer i smarta städer, känner du att interoperabiliteten och sambandet mellan	

		olika aktörer och olika system, ser du att det finns några säkerhetsbrister i detta?	
21	A	Ja, är inte rätt person att uttala mig men jag förstår att det finns problem eller risker i såna övergångar, vi har varit väldigt noga med personuppgiftslagen och den datan som överförs, vi är inte intresserade att riskera den typen av data, integritetsfrågor är centrala för oss. Det vi är intresserade av att göra i en smart stad är att optimera transport och energiflöden till exempel. Och då finns det naturligtvis massa persondata i dom flödena, antingen om det tas upp från mobiltelefoner eller vad det nu är för något. Men, för att kunna optimera system så kanske det inte alltid behövs så mycket individdata, man kanske kan tvätta bort den. Energibolagen kanske gör det inom sitt och sen delar med sig med den informationen som behövs för att optimera sina system. Så den diskussionen pågår definitivt. Att minimera, ja, sen det är en annan typ, det finns många dimensioner i cybersäkerhet, det är inte mitt expertområde, utan jag svarar på det som jag känner till.	K&A-K
22	J	Det gör inget, det är perfekt.	
23	G	Det för oss in på nästa fråga då, har du några ansvariga för cybersäkerhet i staden?	
24	A	Det är vår IT avdelning för Umeå kommun som har det ansvaret. Sen har vi några, sen har vi läsbehörighet och sådär från olika register och liknande som Umeå kommun har. Jag skulle kunna säga att det är i kontakt med en av våra IT-specialister som har bäst överblick av IT-kontoret. Sen finns det säkert andra hos honom, men om ni vill ha en överblick så skulle jag rekommendera att prata med honom.	O-OA
25	G	Brukar de som faktiskt arbetar med cybersäkerhet på IT kontoret, brukar de kallas in vid smart city projekt och ge sin vy av det?	
26	A	Absolut så gör de det, de två stora projekten som vi driver just nu, då det här som heter Ruggedised. Det är vårt stora stadsutvecklingsprojekt just nu, i universitetsstaden Umeå, där är de väldigt mycket fokus kring öppen datafrågorna eftersom att det är det som, väldigt mycket av datan som genereras ligger utanför Umeå kommun, inte allt, men mycket.	

		Så det handlar om att skapa en plattform som är öppen för just samverkan med andra, så det är. Men det andra projektet handlar om IoT-tjänster i fastigheter, där är vårt fastighetskontor ansvariga främst, är inte lika insatt i det projektet, det ligger lite utanför vårt mandat, men dom ligger väldigt nära varandra, vi lär oss mycket av dessa projekten, och där är IT-kontoret mer involverade. De sitter som projektledare för de projekten.	
27	G	Hur ofta brukar det komma upp typ med då IT-kontoret angående cybersäkerheten i smart city projekt?	
28	A	Vi träffar regelbundet IT-kontoret, med vår syster enhet, vi träffas regelbundet men sen, är ju det här egentligen en fråga som inte de behöver, de som är ansvariga för cybersäkerhet behöver inte involvera oss om man säger så egentligen. Jag tror att det finns andra som vet betydligt mer om det här än vad jag gör.	O-OA
29	G	Det är ingen fara.	
30	A	Men ja, det finns absolut såna som är anställda med koppling till det här.	
31	J	Är cybersäkerhet ett ämne som är prioriterat när ni diskuterar strategi vid nya smart city projekt?	
32	A	Ja, alltså, egentligen, just med tanke på att de här smart city projekten har drivits ganska mycket av den här externa finansieringen, det är ju, att, utifrån det så skulle jag säga att, det har diskuterats litegrann, men det har inte varit huvudfrågorna, därför att det är inte så, alltså, våra finansiärer har ställt frågorna, och eftersom det är ett sätt att, det här är ju saker som ingår i vårt ordinarie arbete, så i det ligger cybersäkerhet, sen har vi växlat upp vårt ordinarie arbete i dessa olika projekten, så jag skulle säga att, lite som jag var inne på tidigare, det är. //Samtalet bryts	OI F-CI

33	A	Jag vet inte riktigt var det bröts men det är fråga för staten och EU hur pass viktiga dessa frågorna är, för oss är det, så som smart city projekt är utformade nu så har inte cybersäkerhet varit huvudfrågan, utan det har mer varit interoperabilitet, men jag kan tänka mig att det har blivit lite mer ökat fokus om det här frågorna, vi märker att de är högre på agendan nu än för ett par år sen.	OI
34	G	Okej! Finns det några cybersäkerhetspolicies eller riktlinjer för att skapa medvetenhet inom organisationen?	
35	A	Ja, men det gör det. Vi har faktiskt haft träningar för alla i kommunen med inriktning på IT-säkerhet. Microkurser där man går en utbildning varje morgon via en online kurs där man får göra olika scenario, det är en ganska ambitiös ansats. Och sen finns det naturligtvis övergripande strategier där, frågorna berörs, jag ska ärligt erkänna att jag inte är en expert på den IT strategin, så jag kan inte svara för detaljen kring det men, det finns absolut strategiska dokument och det görs insatser men som omfattar alla anställda.	
36	J	Ja. Är, jag tänker att vi går tillbaka lite, vi hoppade fram en fråga där i tumulten av tekniska problem, men skulle du anse, ser du cybersäkerhet som en del av den övergripande strategin i smarta städer i Umeå?	
37	A	Mja, kanske snarare som en del av det grundläggande. Ja. Skulle jag säga, att det ligger i vårt ordinarie, om man tänker, alltså, det är nog så vi, jag tror inte att jag skulle vilja säga, att vårt utvecklingsarbete har inte varit, jag jobbar mycket med externa projekt, där är det inte fokus då, och det är mycket med tanke på att det inte styrts mot det. När staten utser Umeå till en pilotkommun eller till en smarta städer eller EU gjorde det härom året så är det inte något de har ställt frågor kring. De har inte tvingat oss till att trycka på ytterligare i de frågorna då, utan det gör vi i vårt ordinarie arbete. Sen kan man nästan säga det omvända då, det blir ju ett, när vi ökar takten, när vi gör ett antal nya tester, så ställer ju det ytterligare krav på att vi har ett grundläggande struktur på plats. Det blir lite stresstest på systemet, när man ökar ambitionerna. Och det är väl lite för tidigt att säga huruvida, för vi går väl just nu in i den fasen där vi, där båda initiativen som jag nämnde startade upp för ett år sen ungefär. Så det är först nu vi börjar känna av vilka lösningar som det blir då, och hur det funkar. Jag har ingen anledning till, det är ingenting som kommit fram hittills, som att vi känner - att cybersäkerheten har utmanats, nu. Ingenting som jag känner till åtminstone.	O K&A-NC

38	G	Nej precis, utan det är också någonting som vi känner, det är ganska, det kanske inte är hyperaktuellt även om det är aktuellt men det känns som att det kan bli någonting i framtiden som blir bara mer och mer aktuellt på så sätt.	
39	A	Ja, men den känslan finns ju definitivt i det här att det blir ju också mer och mer komplext i och med att vi, åtminstone har det blivit så hittills i och med att försöka hitta några smarta lösningar kring det här som kan förenkla situationen men just nu så har, det är ju när man öppnar upp för alla de här parterna att samverka, nu tar jag det här öppen data exemplet igen, så blir det ju ett, liksom, en liten förvirringsfas, då.	
40	G	Men jag tänker, det här återkopplas lite till det du snackade innan om, just finansiärerna. I de här smart city projekten då, i budgeten, finns det en kategori för cybersäkerhet eller är den inkluderad i IT budgeten, i projektet?	
41	A	Ja, den är inkluderad. Det är upp till, egentligen, vi tar det stora Ruggedised, på 180 miljoner. Det delar vi med tre, eller två andra städer, där ligger då, en stor budgetpost handlar just om IT infrastrukturen mycket kring datahantering så att där ligger ju - där ligger absolut de här frågorna. Men, känslan är väl att det har varit ganska mycket fokus på att bygga plattformen snarare än att, det är liksom leverabeln om man säger så.	K&A-NC
42	G	Ah, alltså mer fokus på funktionaliteten och inte det underliggande?	
43	A	Precis. Precis. Det är min känsla att det har varit, så var det när vi gick fram med det här, ja men säg att det är två år sen, och vi startade upp det för ett år sen och formulerade projektet tillsammans. Rotterdam, Umeå, Glasgow. Därav namnet Ruggedised. EU akronymer, ja.	
44	J	Okej, så är kostnad ett problem när man, när man så, anser du att kostnad är ett problem när man kollar på cyber security i de här städerna. Är kostnaden en faktor, helt enkelt?	

45	A	Ja, absolut. Ja men, allt utvecklingsarbete kostar pengar och det här är definitivt en sån fråga som vi behöver utvecklas kring. Och det är en av anledningarna till att vi söker de här samarbetena med nationell och internationella samarbetena att vi har inte de, jag menar, kommunerna är ju skattefinansierade, och det ska alltid vägas, för oss så vägs alla satsningar mot andra olika behov, om det är skolan eller vården eller så här. Och när vi identifierar att det här är ett utvecklingsbehov som vi har så är det väldigt ofta som vi hamnar i det att, då vi söker pengar för det här så vi kan göra det. Så bygger man upp ett projekt runt om det. Och det är för att det är en utmaning. Sen är det naturligtvis så att säkerhetsfrågor har en hög prioritering och man kan naturligtvis, det är inte som att vi står och faller med ett projekt blir beviljat eller inte. Men just en del med de här utvecklingsidéerna och tankarna och om det då är en idé vi vill testa, där brukar det generellt sett underlätta med de externa pengarna. Och, men jag skulle inte vilja säga att vi har något, det är egentligen en fråga som du ska ställa till IT kontoret. Om hur de ser på deras grundläggande uppdrag kring cybersäkerhet. Men ja.	F-CI O-BA
46	J	Ja. Anser du att tillräckligt mycket pengar läggs på cybersäkerhet?	
47	A	Jag vet inte. Den frågan kan jag inte svara på. Vi märker ju att det fortfarande är en, att det dyker upp nya, nya utvecklingsbehov hela tiden, alltså att det finns anledningar till att testa nya lösningar och så. Men det kan ju också ha att göra med att det är ett väldigt snabbt område som har utvecklats. Att det är ett område som håller på att utvecklas just nu och därför kommer upplösningar som man behöver fundera omkring och behöva förhålla sig till på olika sätt. Men svaret brukar ofta vara nej, om det är..	
48	J	Så, så som jag uppfattar det så, ni kör på.	
49	A	Oj, nu hör jag er lite dåligt här.	
50	G	Oj, hör du oss bättre nu?	

51	A	Ja, nu hör jag er lite bättre.	
52	J	Så som jag uppfattar det, ni helt enkelt hanterar ni de problemen som kommer när de kommer?	
53	A	Nja, det vill säga, vi har en IT strategi, och där finns det här med att definiera, vi har en plan för att hur man ska hantera det men det är bara det att jag är inte superinsatt i den. Det vi möter av från vår sida, det är just de här - nu finns det möjlighet att göra någonting, det här är saker som vi borde arbeta med. Ja men väldigt konkret vad är det här med öppen data, det är ett sådant område som vi måste kunna hantera på ett smartare sätt än vad vi hade gjort tidigare. Vi såg utvecklingsmöjligheter, det var baserat på då för två år sen, den analysen. Ja, samma sak när det gäller de här IoT-tjänsterna om hur vi bygger upp sensorer i olika verksamheter, fastigheter och så. Det kommer ju ifrån en verksamhets, ett konkret verksamhetsbehov. Om det kommer från en cybersäkerhetsstrategi eller inte, det är jag lite osäker på. Jag vågar inte svara på det. Men jag vet att det har varit, det har inte varit bara inom IT kontoret som behovet har identifierats, utan oftast kommer det från andra aktörer. Kan ha varit, energibolag eller, alltså. Jag vet att det var städservice som hade identifierat vissa behov om hur man städar nya fastigheter på nya sätt. Om hur man styr det på nya sätt.	K&A-K
54	J	Ah, ok.	
55	G	Ja, det är lite, uppskattningsvis då, när det kommer till nästa fråga, men ungefär vilken procent skulle du tro, är det som, läggs på cybersäkerhet i smart city projekt?	
56	A	Hmm. Ja precis. Jag skulle säga att, kanske att ICT komponenten i ett smart city projekt är ungefär en tredjedel. Den är rätt stor. Och sen vad man definierar som cybersäkerhet i den, det är svår. Men, man kan nog säga att liksom, det finns absolut en budget till det och jag tror egentligen att det kanske, jag tror att det skulle kunna styras till att bli mer fokus på de frågorna lite beroende på hur att utlysningarna inte riktigt styrt mot det. Så att, det är litegrann att det blir en definitionsfråga, men finansieringsmöjligheterna har inte styrt mot cybersäkerhet, så kan man väl säga.	F-CI F-NB

57	J	Ja, men du sa att 30 % läggs på IoT, eller ICT, vad..	
58	A	Ja, det är ganska lika, min bedömning är att det är ganska lika fördelningar men alltså. Så som EU kommissionen definierar smarta städer handlar det om att transport, energi och ICT lösningar ska samverka. Och då har vi, för vår del skulle jag säga att det är ganska lika delar.	
59	G	Intressant. Då kommer vi till en annan liten kategori här. Och det är, när ni har de här, alltså, era leverantörer och vad heter det, kontraktörer, heter det det på svenska?	
60	A	Ja, just det. Jag förstår.	
61	G	För att, där, i och med att det finns en hel del aktörer i det här projektet, så då måste man jobba med dem, men hur mycket förtroende har ni för de som ni anlitar i relation till cybersäkerhet då, då?	
62	A	Ja, det är en bra fråga. Man får tänka på hur det definieras egentligen. Man kan väl säga såhär, att vi har ju ett, våra säkerhets.. Hur det där definieras inom ramen, egentligen är det en fråga att ställa till IT kontoret, hur de gör, de som verkligen är inne i de, det är de som gör de upphandlingarna, inte vi. Men generellt så är det ju, vi upphandlar ju enligt lagen om offentlig upphandling och så, så det är ingen - men ja, det är en fråga att ställa till, då exempel Lars Sandström här.	O-BA
63	J	Men, personligen då, känner du att du har tillit till de leverantörerna som..	
64	A	Oj, nu hör jag dig lite dåligt igen.	

65	J	Ja, förlåt. Det är nu när vi bytte mikrofon så måste man vara väldigt nära. Men personligen, känner du att du litar på era leverantörer och liknande, om man bara rakt krasst skulle köra det utifrån vad du anser?	
66	A	Ja, men absolut. Och vi definierar ju.. Jo, men det tycker jag att vi kan säga att vi gör. Det finns en tilltro, men sen är det ju alltid så att det där följer ju, man blir ju uppmärksam när det dyker upp säkerhetsbrister, kanske inte alltid inom ens egen organisation, vad som har hänt. Så att, ja, jag har inte haft anledning till att känna - att ifrågasätta det hos våra leverantörer. De som har haft den typen av uppgifter har vi, som person vet jag att vi har, ja, det har funkat bra. Så att säga. Men, det finns ju också en liten del, jag skulle vilja säga att det fortfarande är en del okunskap också i den egna, även nu i organisationen kring den här utmaningen om vem som hanterar datat om vi lägger det i den offentliga eller privata sfären. Så att det, det pågår ett litet förändringsarbetet internt kring det. Vi har fortfarande upphandlingar som inte verkar i linje med, där vi inte har full kontroll på data och det finns hos andra leverantörer vilket gör att vi inte kan sedan göra de här korskopplingar mellan de här olika dataset och liknande för att skapa, för att skapa samhällsnyttan då. Så att, och där kan vi med en bättre upphandling kunnat göra bättre. Jag tror lösningen, det är den, åtminstone enligt min bedömning.	OS-T OS-C
67	G	Ja det är intressant, för det känns som att det här till viss del uppdelat de olika ansvarsområdena.	
68	A	Ja, så är det ju. Det är väldigt, ja kommunen är väldigt sektoriserad som organisation och sen är vi dessutom väldigt beroende på samarbeten med externa parter. Och vår roll är, det är ju för det här som då till exempel, anledningen till att EU kommissionen är väldigt intresserad av städerna och smarta städer är ju väldigt mycket vår roll som en offentlig aktör nära medborgarna i Europa. Så att det kan vara den aktören som, just utvecklar, ja samhällsnytta tycker jag är ett bra ord. Sen finns det ju affärsnytta också, det är inte i vårt huvuduppdrag att skapa affärsnytta det är jätteroligt för de företagen vi samarbetar med men det är inte det vi är till för. Så att, och där tror jag att - vi märker av att det finns en väldigt stor önskan att många ska vara med och bidra till den här samhällsnyttan och det har varit ganska mycket problem. Om man tar energibranschen till exempel så den privatisering som har gjorts har inte varit i oproblematisk i många delar av Europa. Och där har ju vi många kommunala energibolag till exempel eller statligt ägda energibolag i Sverige som har lite andra, andra förutsättningar att jobba på - andra värden om man säger så.	O-OA

69	G	Du snackade innan om de här, alltså, de offentliga upphandlingarna då då. Men finns det beslutat i just de här, kontrakten och avtalen, klausuler om cybersäkerhet eller informationssäkerhet?	
70	A	Ja, det gör det. Det finns, så all dataflöde, cybersäkerhet följer ju, jag försöker tänka litegrann nu hur det ser ut. Ja, de här kontrakten är ju galet långa, men ja det gör de. Definieras till exempel, en definition till hur vi, att just data ska vara i “the public realm” som det heter på engelska, den offentliga sfären. Så att, och i det ligger det också att det blir kopplat mot personuppgiftslagar och den typen av lagstiftning och sen kommer det in. Så ja, cybersäkerhet, åtminstone indirekt, finns med i avtalen. Sen vet jag inte om det är specifika.. Men det är väldigt, väldigt omfattande avtal.	
71	G	Ja men perfekt. Ja, det var väl egentligen alla våra frågor.	
72	A	Ja. Jag kunde svara, hoppas ni kunde få - det här är inte mitt expertområde så jag svarar utifrån..	
73	J	Ja, men det var exakt det vi var ute efter, så det var perfekt för oss.	

Appendix 2 – Interview 3

Sex: Male

Age: 60+

Alias: I

Date and Time: 2018-05-03, 15:03

Type of interview: Telephone interview

Duration: 31:02

I: Interviewee 3

G: Gustav Jansäter

J: Joel Olsson

#	Speaker		Code
1	G	Till att börja då, undrar jag vilka aktioner som är tagna och om det finns ett tillräckligt fokus på just cybersäkerhet i smart initiativ, smarta städer initiativ?	
2	I	Då ska jag börja med att berätta min bakgrund kanske, min bakgrund är att jag leder en avdelning på miljöförvaltningen i Stockholm och vi behandlar olika typer av miljöprojekt, miljöbilar, miljötillsynen och miljöfrågor i byggandet också. Och just vid klimatarbetet så har vi lyckats halvera vårt utsläpp i Stockholm per capita, men för att komma vidare så måste vi ha nya smarta lösningar som involverar dom boende, eller folks resor, med liksom, tänk och så inte bara tekniska åtgärder, dom tekniska åtgärderna är lågt hängande frukt. Fjärrvärmen, och konverteringen av den, för att göra det så tittar vi på hur vi kan jobba mer med den här typen av åtgärder, och då dök det upp den här utlysningen av smarta städer, smart cities and communities, Horizon 2020. Då satt jag ihop en ansöka efter att ha haft auditions med ett 20-tal städer, bolag, dessutom, kommunala bostadsbolag och så vidare. Då fick vi ihop ett konsortium där 2014 fick vi ihop det sista på våren och till hösten fick jag en hint om att vi var utvalde och sen så startade projektet första januari 2015. Det heter GrowSmarter, så det är mest så jag	

		arbetar med smarta städer och inte så mycket kring cyber eller IT-säkerhet. Då borde ni prata med vår IT avdelning istället egentligen. Men utifrån mitt perspektiv så är det ett projekt där vi arbetar med beteendepåverkan och därför så samlar vi ganska mycket data kring användare. För att göra det, så måste vi också ha deras medgivande, särskilt med GDPR som kommer här snart så måste vi hantera det på ett helt annat sätt än vad vi har gjort förut. Och vi hade till exempel en åtgärd som har handlat om att ta mobiltelefon information, hur människor åkte i bilar och så vidare för att bygga nya trafikplaneringsmodeller, det är ett samarbete mellan telekomoperatörerna och IBM och trafikkontoret i Stockholm. Det fick vi överge det eftersom att telekomoperatörerna inte var beredda längre, dom hade GDPR och hantera vilket blev problematiskt för dem. Så då fick vi istället använda en lösning som använde sensorer, och då mer inriktad på gång och cykel som har fokuserat på vissa områden, som slakthusområdet och Globen vid stora events och samtidigt kartlägga dessa resor. Det har däremot gått att lösa utan identifiering. Sen har vi också försökt att påverka ett beteende om hur man källsorterar sitt avfall och lägger det i olikfärgade påsar och slänger det, då har vi gjort så vi kan se vilka hus som är duktiga på att källsortera och ge olika typer av feedback tillbaka till brukarna, nu har ni sparat så här mycket träd, eller såhär mycket biogas har ni bidragit till genom ett organiskt avfall. Där har vi avidentifierade uppgifter men som ändå kartläggs per trappuppgång. Så att den typen av uppgifter måste vi hela tiden hantera och se till att de hanteras på ett korrekt sätt.	
3	J	Ja det är klart.	
4	I	Sen ser vi till att den typen av data som vi samlar in som kan tillgängliggöras, lägger vi ut i form av öppen data också, inom projektet för att göra möjligt för fler att kunna använda den datan, Det samlar vi in. Där har vi en lång tradition i Sverige av offentlighetsprincipen att data ska vara offentlig även om den kanske inte alltid är så lättillgänglig eftersom det inte är så lättillgängligt.	
5	G	Ja, men det är ju bra!	
6	J	Med tanke på den tidigare forskningen som har bedrivits i detta område, så handlar det mycket om personer i din roll, så det är därför vi	

		vill fråga just dig. Så jag tror det kommer bli väldigt bra. Så vi tänkte börja med en mer generell fråga, och då undrar vi, utifrån din erfarenhet av smarta städer och smarta städer initiativ, tycker du att det finns ett tillräckligt fokus och aktioner tagna för cybersäkerhet?	
7	I	Ja, men det tycker jag.	
8	G	Har du något exempel på något tidigare projekt där ni känner att det fanns tillräckligt fokus så att säga?	
9	I	Ja, men vi har hela tiden fråga angående informationssäkerhet, det handlar hela tiden också om, ibland individrelaterad information och vi tar hela tiden hänsyn till att inte släppa ut sånt som kan hota den personliga integriteten så det har vi hela tiden i all vår verksamhet, det har inte bara med smarta städer att göra utan det har att göra med hur vi hanterar information inom en myndighet som vi är.	
10	J	Ja, intressant, det var mer en allmän fråga.	
11	I	Då fick du ett allmänt svar också.	
12	J	Hehe, då kommer vi in på nästa kategori, eller det kanske inte är så viktigt, men vilka risker ser du med smarta städer initiativ?	
13	I	För det första så är det väldigt svårt att säga generellt, det beror helt på hur man definiera smarta städer och det, det verkar ju ingen riktigt kunna göra. En smart stad verkar kunna vara allt som är lite bättre än något.	
14	G	Precis, det är det vi har uppfattat också, det är ett brett begrepp som många försöker definiera.	

15	I	Ja, det är nästan som värdeord nästan, tidigare var det hållbarhet, hållbara städer som gällde och nu har det blivit smarta städer. Men, en del inom IT-branschen, jag åker till massa mässor och seminarier där jag blir inbjuden att prata om smarta städer och då är det ofta, 95% av dom som är där är från IT-sektorn för att sälja lösningar, och sen är 5% av dom som kommer dit från städer som kommer dit lite storögt och tittar och förstår ingenting, och egentligen skulle man behöva vända på det. Det skulle behöva vara några från städerna som berättar vad dom har för behov och att IT-sidan lyssnar och tar fram lösningar som kan tillgodose de behoven som städerna har. Så att, så att, många som kopplar ihop smarta städer med ICT men det behöver ju inte vara det heller egentligen. Om man tittar på ICT så finns det massor med både risker och möjligheter med den data som hanteras, det finns risker att det ska komma ut sådant som rör individerna och där är ju, det kan man ju se i just GrowSmarter projekten så är man i Tyskland livrädda för smart elmätare. Det har inte gått att få genom den lagstiftningen trots att EU har tagit beslut om att det ska vara infört, men det har dom inte fått igenom eftersom att då skulle någon teoretiskt kunna se att just den kvällen har jag förbrukat lite mer el och då kanske jag var hemma trots att jag sa att jag var någon annanstans, då blir jag avslöjad. Så Tyskland är livrädda för det medan nu vi i Sverige tycker, vad skönt, då slipper vi gå och läsa av mätare och fylla i den där lappen och skicka in. Samtidigt, i Tyskland är det inte samma debatt om någon skriver på Facebook eller om man handlar i någon affär med kort som registrerar vad man konsumerar så att dom kan få mer erbjudande hela tiden utifrån det. Ja, det finns, det finns en väldig ojämn syn på den här säkerheten och vad man uppfattar som säkerhet. Folk verkar vara mer rädda för att samhället ska kartlägga än för att privata aktörer ska kartlägga en, verkar det som, utifrån vad jag har sett, i min erfarenhet.	
16	G	Känner du att det finns en hotbild mot smarta initiativ?	
17	I	Det ena är det här med personlig integritet, där kan det finnas en viss hotbild, men jag uppfattar att folk generellt är väldigt ojämna i riskbild av det som jag tidigare sa, väldigt mycket kartläggs om hur man beter sig när man handlar på internet redan, så det som offentliga kartlägger är rätt lite egentligen i jämförelse med det. Den andra säkerheten är att man får bortfall av information, att, backup system och sånt där fungerar inte riktigt. Det tror jag kan vara nästan ett större säkerhetsproblem. Ett tredje är att man har systematiska fel i data som man samlar in så att informationen blir av låg kvalité. Det måste man alltid också jobba med det. Det är egentligen ingen skillnad på nu och tidigare, det är helt enkelt bara att vi samla in mer data nu för det är lättare att samla in och	K&A-RA

		det är också lättare att lägga in kontroller. Det finns både problem och möjligheter.	
18	G	Okej, vad bra! Sen tänkte jag säga att, har ni någon säkerhetsstandard som ni följer när det gäller informationssäkerhet eller cybersäkerhet?	
19	I	Det har vi säkert inom staden rent allmänt, men det får ju, det får avdelningen för digital utveckling svara för. Inom projektet GrowSmarter så har vi en data management plan, hur vi hanterar vår data, hur vi lagrar den, tillgång, vilka uppgifter som är tillgängliga och på vilket sätt och så, så inom projektet så har vi en data hanteringsplan.	O-BA
20	G	Så ni har alltså lite mer generella övergripande strategier när det kommer till hantering av cybersäkerhet?	
21	I	Det kan man säga.	
22	G	Vid införandet av smarta initiativ, det kan egentligen betyda vilka projekt som helst egentligen, gör ni någon typ av riskanalyser då eller?	
23	I	Ja det gör vi, men analysen kan blanda in andra saker också, i såna här projekt har man massa risk analyser om vad som kan gå fel i projektet, och det har inte bara med datasäkerhet att göra utan det, det är mer att förseningar i projektet och hur påverkar det ekonomin och hanteringen av projektet och så vidare, det är mer sådana risker.	
24	G	Men överlag, finns det många kategorier som behandlar då t ex säkerhetsrisker också när det kommer till cybersäkerhet i den här riskanalysen?	
25	I	Det finns väl enstaka som gäller informationssäkerhet men mer handlar om ekonomiska risker kring projektets eventuella förseningar eller kostnader som kan uppstå eller så.	K&A-NC F-CI

26	J	När du tänker på interoperabilitet mellan olika smarta sakerna ska kommunicera med varandra och de olika aktörerna inblandade ser du några säkerhetsrisker eller brister i det?	
27	I	Det är en svår fråga, för det första så pratas det mycket om interoperabilitet där man tror att allt ska kommunicera med allt, och så är det inte riktigt, det är mer någon slags dröm som tekniker har, ta en sån sak som smarta lyktstolpar med LED och sensorer som är dimmade när det inte är någon där men tänt till full belysning när det kommer någon. Där finns det tydligen fyra olika typer av mjukvarusystem som säljs, jag är inte säker på att dom är helt interoperabla med varandra men, men i samband med att man gör mer och mer upphandlingar i det offentliga så kommer det kräva att dom kan samverka, så att man inte blir inbunden till en leverantör. Det är ett exempel. Den smarta lyktstolpen sen, det samverkar inte med det smarta hemmet eller vad som helst annars, utan den är sin egna lilla del och där fanns det fyra olika mjukvaror och leverantörer, i smarta hem finns det kanske tio olika leverantörer och så vidare. Så att, jag tror inte att, det finns dom som tycker att man ska göra någon typ av gemensamt system och sätta sig vid ett skrivbord och tänka ut ett gemensamt system för allting, det kommer jag inte kommer komma. Det är som att säga att allting ska standardiseras till en standard, en standard för allt, och så enkelt är inte världen. Jag tror att man kommer närma sig mer standarder för olika produkter både när det gäller mjukvara och hårdvara i med att marknaden efterfrågar det. Vi kan ta ett annat exempel, mobiltelefoner och deras laddare, nu har vi i alla fall USB som är strömstyrkan men det är inte så att dom har samma ladduttag så att säga, dom är likadana, men det är samma strömstyrka, och det tog 20 år eller något sånt så att. Man ska inte överdriva tron om att allt det där går att lösa i ett nafs men upphandlingar kommer driva det och konsumentmakt kommer driva utvecklingen mot mer interoperabilitet.	K&A-K K&A-NC OS-C
28	J	Om man kommer dit, skulle det finns några risker då?	
29	I	Det finns kanske en risk att man faller till ro och inte utvecklar lika mycket som om det finns konkurrenter, om det bara hade funnits Microsoft och inte Apple så kanske PC hade stagnerat mer medan Apple har nu drivit på, Windows 10 ligger mer likt iOS som operativsystem det är väl en sån utveckling, där det, om det finns två stycken som konkurrerar med varandra. Så jag tror att det är bra, jag tror det är bra	K&A-K

		kanske med några konkurrerande till och med, men gärna att dom är interoperabla.	
30	G	Jag tänker på, den här IT-avdelningen som du nämnde, att det var de som höll på med just säkerhet och liknande, brukar de tas med i de här smarta initiativen, brukar dom vara gemensamma beslutstagare?	
31	I	Jag kan säga, inte direkt i projekten det är de sällan, däremot är de med när staden bestämmer sig för olika plattformar. Vi håller på att införa en gemensam IT-plattform nu, vi har haft Volvo som blev HCLIT som har driftat 60000 datorer i staden och hela systemen kring det och nu har det gjorts en ny upphandling med en ny leverantör och när man gör såna plattformar, system för hela staden, då är dom garanterat med. Så det är mer på den nivån, och med ekonomisystem och personalhanteringssystem och gemensamma system i hela staden, där är man med. Men i enstaka projekt så finns inte digital utveckling med, utan kanske som observatörer ibland, vi kanske få frågor om något som vi undrar över och så.	O-BA O-OA
32	G	Vid, när man tilltänker dessa smart säkerhetsprojekten, brukar cybersäkerhet få plats och diskuteras vid, när det kommer till strategi?	
35	I	När vi skrev ansökan så tog vi upp vissa informationssäkerhet och sen också väldigt många andra risker så det finns ett avsnitt som risker när vi skrev ansökan också med de kontrakt som vi har med EU-kommissionen. Varje projekt som har sökt från EU har ju behövt beskriva det men inte sen varje, vi har typ ett femtiotal measures inom varje projekt och där beskrivs vart en av dem är. Mer på en aggregerad nivå.	
36	J	Så, finns det någon typ av såhär, cyber säkerhetspolicys eller projekt för att skapa medvetenhet och så för anställda inom organisationen, så man lär ut vilka risker som finns och så vidare?	
37	G	För att öka medvetenheten i organisationen.	

38	I	Om vi tar, uppgifter om personuppgifter så har hela organisationen genomgått en enorm inventering när det gäller allt med GDPR, vi har inventerat alla processer och alla uppgifter som används där. Så där är ett väldigt omfattande arbete som pågår nu.	
39	G	Hur är det när det kommer till då ett säkert arbetssätt?	
40	I	Det beror på vad man menar med säkert arbetssätt, jag skulle säga att vi jobbar mycket mer med att kvalitetssäkra våra arbetsprocesser och vilken information som används där. Ibland skulle vi också behöva lägga lite mer tid på att effektivisera våra processer, det vill säga att man måste göra en avvägning mellan kvalite och kostnad. Hittills har vi varit väldigt duktiga på att höja kvaliteten.	
41	J	Då kommer vi in lite på nästa segment här och det handlar om, om ni budgetar för cybersäkerhet i dessa projekten?	
42	I	Inte mer än vad jag har beskrivit hittills. Att informationssäkerheten finns med som en del, men det finns väldigt många andra risker som vi betraktar som större och mer omfattande. I såna här projekt så får vi 25 miljoner euro, det vill säga en kvarts miljard för projektet och då gäller det att vi ser till att projektet går smidigt och kommer fram, så vi får ut den finansieringen också som är tänkt, så det är en rätt så stor ekonomisk risk som vi tar också med såna här projekt. Det är väldigt viktigt att hantera tidsplaner och komma förbi eventuella förseningar och så.	A&K-NC F-CI
43	G	Så det är mer fokus på funktionaliteten och att införa dessa?	
44	I	Ja det skulle jag säga, det är ett fokus på funktionalitet.	
45	J	Så är kostnad en faktor när man tänker på cybersäkerhet i såna här initiativ?	
46	I	Vår kostnad för cybersäkerhet?	

47	J	Ja precis, är kostnad ett problem eller en faktor?	
48	I	Ja, kostnad är en faktor till allting, både för cybersäkerhet och kvalité och övrigt, så man måste hela tiden väga mot kostnad, det är därför vi ibland skulle behöva titta mer på kostnad och funktionaliteten bara för att höja kvaliteten hela tiden.	
49	G	Har det funnits tillfällen där det har blivit prioriterat, där det har blivit bortprioriterat med just cybersäkerhet för att införa funktionalitet?	
50	I	Nej det skulle jag nog inte säga heller riktigt. Men jag kommer i alla fall inte på något tillfälle där vi verkligen behövde göra en sådan avvägning. På andra sidan så på våra riskanalyser så har inte cybersäkerhet av allt varit det som har kommit högst.	A&K-NC
51	J	Så anser du att tillräckligt mycket pengar spenderas på informationssäkerhet/cybersäkerhet i dessa projekten?	
52	I	Ja, det tycker jag. Är en svår fråga men jag tycker ändå att vi har gjort en bra avvägning mellan dessa delarna.	
53	G	Det är också en lite knölig fråga, men ungefär hur mycket pengar läggs i procent på ren cybersäkerhet?	
54	I	Ja, det är svårt men under 5% i alla fall.	F-CI
55	G	Du nämnde tidigare Tieto och andra leverantörer på så sätt, så tänkte vi fråga, hur mycket förtroende har du för dessa leverantörer i just smarta städer projekt?	

56	I	Hur stort förtroende jag har för dom leverantörerna som vi nyttjar?	
57	G	Ja när det kommer till deras cybersäkerhet och informationssäkerhet?	
58	I	Ja, då skulle jag säga 4 på en femgradig skala.	
59	G	Sen tänker jag mig att det är en hel del, offentliga uppköp, men jag tänker finns det i dessa avtal och liknande med era leverantörer, finns det klausuler som berör just cybersäkerhet eller informationssäkerhet?	
60	I	Dom som är med i projektet är bundna till avtalet med EU-kommissionen, där är det 172 sidor och tio punkter, det är rätt så omfattande och där finns det riskanalyser gällande data och personuppgifts säkerhet intaget i den texten. Så alla parter är bundna av det. Till det finns det också konsortialavtal som reglerar risker och så vidare, men även andra risker som intellektuell property rights, vad heter det på svenska? Patenträttigheter, material rätt och, och det är har då varit stora diskussioner kring det, för några trodde kanske att dom skulle uppfinna en massa inom projektet och hur skulle dom uppfinningarna kunna hanteras, utan att projektet egentligen är inriktat på att uppfinna något nytt utan det var kanske mer att använda nya tekniker, så det tycker jag var lite överdrivet. Så att, vi har avtal som reglerar det här ganska väl och mycket annat.	
61	J	Och det utgår mycket då ifrån vilka krav som EU eller de som finansierar ställer?	
62	I	Ja precis, de ställer krav på hela ansökan i en kontraktsbilaga.	
63	G	Är det också lite kopplat till det som du berättade innan, att det finns ett stort fokus på funktionaliteten?	

64	I	I dessa avtal så är det väldigt viktigt att säga att, att dom risker som vi ser är väldigt mycket annat än cybersäkerheten. Det är också beskrivet i de riskanalyser som finns i avtalet.	K&A-NC

Appendix 3 – Interview 4

Sex: Male

Age: 40+

Alias: C

Date and Time: 2018-05-04, 13:00

Type of interview: Telephone interview

Duration: 35:45

C: Interviewee 4

G: Gustav Jansäter

J: Joel Olsson

#	Speaker		Code
1	C	Vi har ju staden, eller i Stockholm trycker vi då på medborgarfokus, och företagsfokus, så att det ska var något som gagnar deras nytta. Så att det inte fokuseras på infrastruktur, eller framkomlighet för trafik så att vi försöker bjuda på - vi ska se skillnader för människorna.	
2	G	Intressant.	
3	J	Ja men det är alltid roligt att se hur alla ser på det olika. Men vi har lite frågor då som vi har som vi tänkte köra igenom. Så första frågan är, upplever du att inom så här smart city initiativ i din, i Stockholms stad - att det finns tillräckligt fokus och aktioner tagna kring cybersäkerhet?	
4	C	Om vi säger så här, vi är i en linda. Strategin för Stockholm för en smart och uppkopplad stad togs 2017 i april. Så vi har ju egentligen, sen strategin antogs i kommunfullmäktige, så började vi att implementera det här programmet första november. Så vi har ju inte jobbat så riktigt länge, men alltså kopplat till vårt program så har vi ju också en aktion med informationssäkerhetskompetens. Det vi pratar om är ju att	OI

		det redan att ta fram en projektplan för de olika projekten, att vi har med oss säkerhetsfrågorna inte bara informationssäkerhet utan även andra säkerhetsfrågor i arbetet. Men arbetet där är det lilla, vi har ju inte kommit så mycket längre i det här programmet.	
5	G	Ah ok, intressant. Och lite så här, när man kommer till smarta city initiativ då då, ser du några potentiella risker när det kommer till cybersäkerhet eller informationssäkerhet, personligen?	
6	C	Nej, det är integritetsfrågan, minst sagt. Där, om vi säger så här, i dagsläget så har vi fem projekt kopplat till varandra, och alla handlar om just plattformstänket. En plattform som ska vara något vi bygger våra tjänster gentemot. Och utifrån den plattformen så får vi då data, som vi ska använda för andra beslut eller för kollektiva beslut eller för politiska beslut. Och i dagsläget har vi tre stycken projekt som, hur liksom verksamhetsprojekt - det handlar om smarta lås, det handlar om smart belysning och den tredje om trafikstyrning. Om vi då kollar integritet så kanske då det här smarta lås som är, det blir mest intressant ur det perspektivet. Alltså, hur hanterar vi säkerhet eller den integriteten för den personen som bor på det stället där vi går in eller som kan behöva stöd och då pratar jag hemtjänsten eller något som vill använda sig av smarta lås. När det gäller smart belysning och smart trafikstyrning så är det som så att att, jag vet inte riktigt i dagsläget vilka typer av sensorer som det är vi kommer använda oss av i de här tjänsterna. Är det kamerasensorer som vi behöver, då har vi alltid det perspektivet som - det är inget nytt. Det har ju funnits under många år. Och sen, sen tror jag att - vad är det för frågor som dyker upp och kan de registrera, på vilket sätt hanterar vi den information vi får? Och det här är ju någonting som diskuteras hela tiden i våra olika projekt. Alltså man kan ju i vissa fall registrera information på individnivå - det vill vi ju inte lyfta upp som öppen data utan då är det snarare - kan vi lyfta upp information på kollektiv nivå? Som andra kan använda sig av. Vi har hela tiden en diskussion om det här, just i våra arbetsprocesser. Hur vi hanterar säkerhetsfrågor.	
7	G	Aha ok. Men du känner inte att det finns någon slags hotbild när det kommer till smarta initiativ, eller?	
8	C	Nej, det gör jag inte just nu. Sen så försöker vi också hantera lite, vad är det för saker och ting som kommer att uppstå i den här - under den här resan? För att vårt sätt, för att veta att vi gör rätt så har vi också, el-	K&A-RA

		ler vi håller på att etablera ett etikråd, som kommer bestå av representanter från olika delar i staden. Där vi då kan, när vi börjar fundera runt om det och om det är så att vi då känner osäkerhet eller bara vill lyfta upp hur vi ska arbeta så tar vi upp det i etikrådet så att de kan komma med en kombination av hur vi bör gå vidare. Vill man ställa det gentemot att man, bara för att det är juridiskt rätt så behöver det inte vara etiskt rätt.	
9	G	Nej precis.	
10	J	Ja. FInns det några såna säkerhetsstandarder som ni följer? I såna projekt?	
11	C	Det finns det säkert, men det är inte något som jag känner till. Alltså, jag är relativt ny i det här projektet. Men vi har ju säkert, eller vi har ju personer som har informationssäkerhetskompetens som finns med i, hela tiden. Och det tror jag säkrar, att vi har den personen med redan från början av projekten säkerställer att vi är på rätt väg.	K&A-K
12	G	Aha, verkligen. Och då då, följer ni då några mer övergripande säkerhets - alltså, strategier eller?	
13	C	Det finns ju rutiner i Stockholms stad som vi måste följa.	
14	G	Ah ok.	
15	C	Och den är ju intressant, den där - om du lyfter den så finns det regler om hur man ska förhålla sig. Men det finns ju också den nya tekniken sätter ju en del av dessa regler på spel. Att man måste följa, hur är lagstiftningen - behöver lagstiftningen förändras på något sätt? Jag har ju inget sånt säkert perspektiv men det jag har lärt mig för någonting så finns det något som heter konsumtionsrätt när det gäller el till lyktstolpar. Så att då den här lyktstolpen med belysning, den får bara, så finns det regler för att i den lyktstolpen får det bar afinnas el till själva belysningen. Nu kanske du ser att, tänk om vi nu sätter upp en lyktstolpe	

		som har ett antal sensorer på sig som kan registrera att, ja, mörkrets inbrott, eller sådär så att den kan dimra ned eller om det kommer någon som passerar. Då behöver ju de sensorerna styras av el och då får de ta det från den elen som ska till belysningen. Och det är ju såna här saker som kan ställas på sin spets nu. Just den här konsumtionsrätten tror jag är från, ska inte säga något exakt, men det är nästan hundra år tillbaks i tiden va. Det finns saker och ting som, ja, kommer få sättas på sin spets när ny teknik ska appliceras.	
16	J	Ja, så - genomför ni någon typ av riskanalys när ni gör sådana här projekt.	
17	C	Ja, det gör vi. Vi kommer genomföra riskanalyser flera gånger under projektet och hela tiden tänka på, det är ju en del man gör i informationssäkerhetsarbetet och jag tror att vi pratar om att göra varje delprojekt kommer vi göra tre riskanalyser på, på informationssäkerhet. Alltså, inledningen av ett projekt, upphandling - vid upphandling då och sen även vid införandet.	
18	J	När man tänker på så, interoperabilitet mellan olika , ja vad heter det, devices, system och aktörer - ser du några säkerhetsbrister där, eller eventuella problem?	
19	C	Ja, det som vi ser, alltså i Stockholms stad så har vi ju ett antal system som har väldigt mycket information om individer. Och där är det viktigt att den informationen är på rätt ställe. Den ska ju inte lämnas ut, på individnivå. Sen kanske det finns tillfällen då vi kan använda den på någon aggregerad nivå. Alltså, vi har ju information om hur många anställda det finns i staden, vilka yrkesgrupper som finns.	
20	G	Så att då, då hoppar vi nästan in eller över nästa.	
21	J	Vi kan ställa den ändå, för formulärets skull.	
22	G	Ja, men, ni hade alltså en i projektgruppen som då jobbade med specifika cybersäkerhetsfrågor då då?	

23	C	Ja, det beror på vad du menar med cybersäkerhet, för det är ganska vitt begrepp. Men informationssäkerhet, ja där har vi en person. Sen cybersäkerhet, det är mer hur vi liksom säkrar våra system gentemot hackning och såna saker. Och det är, nu spekulerar jag lite, men jag antar att det är något sånt vi behöver upphandla när vi köper plattformar. Vi köper drift av plattformar, det är inte sånt som vi jobbar - eller det är inte sånt som vi gör i Stockholms stad, utan vi köper de från de leverantörer, eller att de ska leverera de systemen.	OS-C OS-T
24	G	Men, så cybersäkerhet är alltså en, eller informationssäkerhet också då då, är ett prioriterat fokus då då, när ni diskuterar?	
25	C	Det är jätteviktigt, vi har alltså blivit utsedda för attacker hela tiden och där behöver vi ha väldigt bra leverantörer som kan det. Och där har vi ganska stor fördel av att var en storstad, som kan trycka på de här aspekterna i högre grad än vad många andra mindre kommuner kan. Gissar jag, ja.	
26	G	Men det är alltså, är det inkluderat i verksamhets, i ert verksamhetsområde också då att cybersäkerhet alternativt informationssäkerhet?	
27	C	Ja det är ju en viktig del att upphandla, va. Vi jobbar ju inte så mycket med egna system, utan vi köper ju de flesta sakerna utifrån och då behöver vi ha kompetens för vad det är vad vi ska ha för något system. Vi måste veta hur vi ska upphandla, att vi har en rätt upphandlingskompetens, när det gäller cybersäkerhet till exempel, så att - det är en viktig aspekt för oss.	
28	J	Har ni någon typ av cybersäkerhets- eller informationssäkerhetspolicy eller projekt för att skapa medvetenhet hos anställda, med träning och liknande? Inom organisationen.	
29	C	Ja det har vi ju. Sen vet jag inte hur bra det är. Visst finns det människor som inte följer våra riktlinjer i en stor organisation, vi har 70000 anställda och vi kan väl säga att, även om svenskarna i hög grad är	O-P

		kompetenta så har vi ju sett hur människor använder sig utav e-post system som inte är godkända eller använder, ja, hanterar saker på och ting på kanske inte på det absolut säkraste sättet. Med sina USB-sticker och sådana saker. Det kanske inte känns som jättestora risker men det finns ju där helt enkelt.	
30	G	Budgeterar ni något specifikt för cybersäkerhet i smarta projekt då?	
31	C	Nej, det ingår ju som en självklar del, va. Om man säger så här, ett smart projekt består av väldigt många delar - vi har ju en infrastruktur del där vi pratar om plattformar och där har, man upphandlar en säker plattform. Vi kommer ha ett styrsystem som styr de här smarta låsen och då behöver vi upphandla ett styrsystem som har hög säkerhet. Sen kanske vi upphandlar ett verksamhetssystem som ska tala om för dem vilka det är till som, som ska jobba med de här personerna och behöver komma hem till dem vissa tider. För att kunna öppna de här låsen, de behöver också ha, då behöver vi ha ett verksamhetssystem som har en hög säkerhet som inte kan hackas. Så att det, vi lägger pengar på cybersäkerhet - det är en självklar sak som ingår i alla olika delar som vi jobbar med.	OS-C F-NB
32	G	Intressant. Men så då är det ingen riktig faktor, i så fall, kanske - kostnad är då ingen faktor för just cybersäkerhet, då eller?	
33	C	Det finns säkert såna siffror men jag, det är ingenting som jag kan säga direkt på rak arm att så här mycket kostar det eller så. Ja, det kostar och vi tänker på det i våra upphandlingar.	
34	G	Känner du personligen att det är tillräckligt mycket som spenderas på, för att säkra system och enheter och liknande?	
35	C	Jag kan väl säga att det är inte så himla ofta vi blir utsatta för - det händer ju titt som tätt att det blir någon sån här cyberattack som får våra system att gå ner. Men, kan det vara en gång per halvår? Det är som sagt olika organisationer utsatta för. Och sen är det väl som alla verksamhetssystem, man behöver uppdatera de hela tiden - för säkerhet och så. Var det Twitter senast, igår va?	

36	G	Ja, det var igår ja.	
37	J	Så du anser då att det spenderas tillräckligt mycket pengar för de problem ni har då på cybersäkerhet?	
38	C	Ja, det tror jag.	
39	J	Man får gissa lite såklart, men hur stor procent anser du spenderas på cybersäkerhet i såna här projekt?	
40	C	Jag har ingen aning. Det skulle bli fel om jag säger en siffra.	
41	J	Ja, det såklart. Den är lite klurig.	
42	G	Men, som vi snackade om innan, just att ni har många leverantörer och kontraktörer där ni, ja, får tjänsterna inköpta då då, hur mycket förtroende sätter du på era leverantörer och kontraktörer?	
43	C	Ja, det där är en jättebra fråga, för att vi har ju - många stora leverantörer, de har man ju kontinuerlig leverantörsdialog med. Och den brukar ju vara väldigt bra. Alltså det, de som får leverera till Stockholms stad det är oftast stora företag som ser en, ja, de är stolta över att leverera till Stockholms stad - det är en stor… Man tjänar sina pengar på Stockholm. Och då behöver man ha en bra dialog. Man vill vara en god leverantör för Stockholm också. Svårare är det, vi har kanske också mindre leverantörer ocks. Det är en stor stad som behöver många olika tjänster och mindre företag som har svårt att kanske matcha de krav som ställs. Jag skulle kunna tänka mig att det var svårare för att driva igenom förändringar i de system och då kanske det inte är just någon viktig information som finns i dem systemen.	

44	G	Men du känner att det finns en tillräcklig tilltro för leverantörerna när det gäller då just cybersäkerhet?	
45	C	Ja det vill jag nog påstå att vi har goda samarbeten med de leverantörer vi har.	
46	G	Ok. Perfekt. Och du nämnde då de här, vid de hr uppköpen då, som sagt, offentliga uppköp och liknande, de här avtalen och kontrakten som skrivs med leverantören - finns där klausuler som just har beröringspunkter med informationssäkerhet alternativt cybersäkerhet?	
47	C	Jag förutsätter det. Jag har inte varit med i någon upphandling utav någon större, men visst måste systemen vara säkra, jag har varit med i arbetet med att upphandla en plattform för hela skolan som innehar alla elevinformation och där har det varit oerhört viktigt att den informationen som finns, både de av elever som, så att säga vanliga elever och de elever som är skyddade identiteter, de är oerhört viktiga att de, att systemen är säkra för alla individer. Så att det finns självklart med.	
48	J	Har du något mer att tillägga på någon fråga, eller något som du känner att man har missat kring detta. Generellt.	
49	C	Nej, men jag tror alltså - alla är ganska medvetna om säkerhetsfrågorna och informationssäkerhetsfrågorna i de upphandlingar och det arbete som genomförts. Där har vi arbetat ganska centralt med hög kompetens så att vi prioriterar de frågorna. Jag tycker ibland att tekniken går väldigt fort det gäller att hela tiden vara på topp och hänga med där.	
50	G	Men är det något initiativ som har tagits från en lite högre instans, att det just ska bedrivas ett arbetande just i hela organisationen för ett högre, en högre cybersäkerhet eller eller informationssäkerhet?	
51	C	Ja just nu pågår det intensivt arbete med just GDPR som är egentligen en del av det här arbetet också. För att säkerställa att man både arbetar med den personliga kompetensen i vår organisation, att vi gör rätt. Så	

		att vi hanterar frågor på rätt sätt. Tekniken i all ära, men om inte människorna som använder tekniken förstår vilken, vad som kan ställa till med, så är ju det, det är ju en lika stor riskfaktor då. Det kan man nog ta med här, att vi behöver ha - vi kan inte förlita oss alltid på tekniken, utan också se vad man kan - vad kan varje individ ställa till med om man gör fel.	

Appendix 4 – Interview 5

Sex: Male

Age: 40+

Alias: O

Date and Time: 2018-05-04, 10:05

Type of interview: Telephone interview

Duration: 44:13

O: Interviewee 5

G: Gustav Jansäter

J: Joel Olsson

#	Speaker		Code
1	G	Ja, finns tillräckligt mycket fokus på just cybersäkerhet i just de här smarta initiativen?	
2	O	Ja, då ska vi se, om vi nu ska tänka vad vi kan göra, eller vad vi har här, som måste kunna klassas som smarta initiativ, ja, är det så här, tänker ni direkt olika app funktioner och sådana saker eller även andra insatser där produkter eller annat till anställda där IT sidan kommer in?	
3	G	Ja, det är väl lite mer generellt - i Lund har de till exempel något initiativ med att införa smarta papperskorgar bland annat och de har ju WiFi och sensorer.	
4	O	Ja, vi ska se här, där, vi kan väl säga som så här, på den sidan där jag jobbar vilket är hållbart resande, där har vi väl inte så här, från kommunens sida har vi inte så mycket sådana här insatser, vi har några på gång - i alla fall så har vi en app som är under utveckling för att, ja, locka folk att cykla mer eller pendla mer på ett hållbart sätt och så där.	

		Men den är under utveckling, den skulle ha varit klar här för ett tag sedan men tyvärr då, det har varit lite produktionsproblem med den. Så att den är inte sjösatt så där kan jag inte säga så mycket om den, än så länge. Vi har också under diskussion här att vi ska, att vi ska eventuellt då få in en app i vår kommande resformsundersökning (?) - men den görs nästa år. Och då ska vi göra en kombination av vanlig pappersenkät men sen även få in information då via en spridd app till kommuninvånarna och se vad det ger helt enkelt. Där har vi inte heller kommit någon vart egentligen, så där kan jag inte heller säga så mycket. Sen, ja det är ju frågan om, man kan inte säga att det handlar mycket om smarta initiativ på det sättet. IT säkerheten har vi jobbat upp ganska mycket när det gäller våra förmånscyklar och sådana saker som vi erbjuder våra anställda i kommunen då. Där det, där det liksom har blivit ett ökat behov av kryptering och sådana saker som kommit till och nu i och med GDPR så, så har det blivit en ytterligare skärpning av hur det här materialet ska överlämnas och hur det ska hanteras och så där. Så att det är en klar förändring verksamhetsmässigt. Däremot så är det ingen funktion som används så dagligen av kommuninvånare eller kommunanställd. Och, ja det är ju inte heller någon - vi har en pågående kampanj som vi har kört sen 2013, vilket är en kampanj då som heter “Inga onödiga bilresor” i den så får kommuninvånare eller folk som arbetar i kommunen de får gå in och ansöka om att då låna elcyklar på veckobasis. Nej, men det är ju då som sagt, kommuninvånare kan ion och boka elcyklar på veckobasis och där ser vi till att, ja i samband med att de tecknar det här, eller skriver upp sig för lån av elcykel att de godkänner att vi använder deras uppgifter och så. Så att vi håller ryggen fri, eller vad man då ska säga, så att de är medvetna om att de måste ställa upp på vissa kriterier. Men där är det heller ingen, så att säga, ingen funktion direkt annars i någon app eller liknande som ska leda till ett ökat hållbart resande, utan här handlar det rent om att få folk att testa de här produkterna då då. Så att, ja, där kommer vi inte riktigt in på någon säkerhetstyp att - vi gjorde en utvärderings, eller vad ska man kalla det, en enkät som heter Shift där Trivector som utför den här, om de gör den varje år eller vartannat det vet jag inte, men hur som helst, så ställer man upp, man skriver upp i den här enkäten som kommun då, vad man gör på olika sätt för att få till ett ökat hållbart resande. Och där kommer frågor om, då kom det här med smarta lösningar och annat om hur vi jobbar med det på olika sätt. Tyvärr så ligger vi ganska lågt där, jag tror att andra kommuner har kommit betydligt längre än Jönköping så.	
5	G	Jag tänker då, med den här appen då till exempel, då sparar den personlig information då som ni då använder.	
6	O	Ja, du tänker den här cykel, eller vad ska man säga, den här pendlings appen. Ja den samlar information om när du ska färdas på ett visst sätt	

		eller när du färdas på ett visst sätt och vilken fordonslag som gäller. Den ska förhoppningsvis kunna känna av vad det ska vara för hastigheter och stopp och annat och känna av ungefär vilken färdslag då. Hur bra det här sen kommer funka, det vet jag inte. Det får vi se.	
7	J	Men, trots att det är, ja men jag tror att de projekten, eller det projektet kan passa bra in på det som vi är ute efter, så att vi kanske kan ha det lite som en referensram då, jag tror ändå att det ska passa.	
8	G	Ja, givet att man måste säkra just den information som finns lagrat på er sida.	
9	O	Ja, där så, tyvärr där får jag göra er besvikna. Som läget ser ut så där det inte jag som jobbar med den appen. Nej, men det är min kollega som har hand om den appen och det är han som har mest information om just den, men han är ledig idag och han är inte här på hela nästa vecka, så att - och ni är i slutfasen av det här projektet, va? Eller hur låg det till?	K&A-K
10	G	I och för sig, lite i slutfasen är vi, men sen tycker jag inte det är några större problem i och med att du har ju insikt i smarta städer och vilka initiativ som tas egentligen, generellt. Det ska inte vara några större problem.	
11	J	Nej, det är inte egentligen så, det är inte så specifika frågor, utan det är mer generella frågor som kommer komma.	
12	O	Ja, men vi kan ju testa så kan vi se vad jag, om det är något som jag inte kan svara på. Vi får ta det som det kommer.	
13	J	Exakt.	
14	G	Men ja, vad tror du - vilka potentiella risker ser du med smarta initiativ när det kommer till informationssäkerhet eller cybersäkerhet?	

15	O	Ja, det är väl den personliga integriteten väl en, en stor bit att tänka på hur man kan skydda den på olika vis. Det ställs vi redan för idag då i och med GDPR. Nej, det är någon -. Det är det riktigt stora biten. Att vi helt enkelt inte bryter mot några lagar eller regler.	K&A-RA
16	G	Känner du att det finns någon extern hotbild just, mot just smarta städer?	
17	O	Ja, om man låter de smarta delarna vara mer styrande så är det ju klart att kommer man åt de systemen så blir det ju mer känsligt. Just för vår del så kanske inte riskerna är så stora, vi är ju inte inblandade i den än, det där, det där det är så mycket drift det handlar om. Vi ser mer på beteendeförändring och sådana saker, och där, jag vet inte, om någon skulle mata in något i några appar eller liknande att folk ska ta bilen istället för att cykla, det är inte riktigt vad vi vill, men det är ju ingen katastrof om någon skulle göra det, kan man säga.	K&A-RA
18	G	Följer ni några, alltså, säkerhetsstandarder när det kommer till införandet av smart city initiativ?	
19	O	Nej, det kan jag inte riktigt svara på hur det ligger till. Det är inte riktigt mitt bord. Nej, just den biten är inte riktigt mitt bord, där har vi en IT avdelning som får ta de beslut som behöver tas när det gäller, vad ska man säga, de produkter som vi använder på olika sätt och hur de blir säkrade på rätt vis.	K&A-K O-OA
20	J	Har ni någon så här, övergripande informationssäkerhet eller cybersäkerhetsstrategi i Jönköping?	
21	O	Det skulle jag gissa på i alla fall, jag törs inte svara på rak arm. Vår IT avdelning är ju, de brukar vara på tå på alla möjliga olika sätt, och jag skulle tippa på att det finns något sådant även här.	K&A-K O-OA
22	J	Så, vi går vidare tycker jag då. Gör ni någon typ av riskanalys när det kommer till smarta projekt? Till exempel ni har ju lite på gång som ni	

		gärna vill göra och så, finns det någon riskanalys som görs i samband till det?	
23		I sammanhanget, nej, det är frågan om det görs. Nej, det tror jag nog vi kan säga att när det kommer till den här appen så har vi inte riktigt gjort någon riskanalys, det har vi nog inte.	K&A-RA
24	G	När man tänker på, när det kommer lite till framtiden så att säga, just många olika smarta initiativ, och många olika system kommer in i bilden - om man tänker då på interoperabilitet, hade du sett några problem eller risker med just större integrering av olika system och projekt?	
25	O	Ja, om man säger så här - vi har haft lite, när det gäller till exempel våra förmånscyklar så har vi haft en extern aktör inblandad och där hade vi behövt någon form av integrering av våra system för att det ska, leveransen av våra skyddade personuppgifter ska se på ett så säkert sätt som möjligt. Sen är jag inte rätt person att svara på det, det här blir ju en säkrare överlämning av personuppgifterna. Där litar jag på vår IT avdelning när de säger att det ligger till på det här sättet, sen vet jag inte om det ökar möjligheterna för externa aktörer att komma åt våra, vårt material eller inte, men då är jag inte rätt person för att svara på det.	K&A-K O-OA
26	G	Så du nämnde då IT avdelningen, är det då de som har hand om cybersäkerhet och liknande, alltså sådana frågor?	
27	O	Ja, det måste vara så för oss. Jag skulle kunna tänka mig att det ligger hos IT en hel del, möjligtvis något hos våra kommunikatörer, informationsavdelningen eller vad man ska säga på kommunen. Men antagligen så ligger ju det mesta här hos IT så.	O-OA
28	G	Jobbar de nära er i just smart initiativ?	
29	O	Nej, det kan jag inte påstå, vi har dock inte kommit så långt när det gäller smarta initiativ men jag vet att det är några saker, tekniska kontoret här till exempel har några papperskorgar som signalerar att dom	O-OA

		är fulla, och vilken status som dom befinner sig i och sådär. Sen är det väl lite andra saker som belysning och annat, dom blir smartare och smartare kan man säga, det gäller säkert många andra saker också men det är inte, det är inte så mycket av det som jag pysslar med som har varit smartare på det sättet kan man säga. Det kommer det antagligen och bli mer och mer av, men inte än så länge.	
30	G	Är cyberbersäkerhet en prioriterad faktor när det kommer till att diskutera nya projekt i smart städer?	
31	O	Jag ser det som en prioriterad faktor, sen, sen som sagt, när det gäller just smarta städer så är vi ju, vi har helt enkelt andra som arbetar i kommunen mer rakt med det. Det finns ju ett och annat projekt, utvecklingsområdet i staden, det hetaste utvecklingsområdet i staden just nu är Södra Munksjön Utvecklings AB. Det är det södra Munksjöns utvecklingsområde, och där, det här är ett område som antagligen kommer att integrera denna typen av lösningar mycket mer, eftersom att det byggs på scratch på gammal industrimark. Den används för att bygga stad, och här byggs det ganska mycket och det finns, det finns mycket planer för framtiden och där skulle man möjligtvis kunna se om man kunde få fram mer information eller om ni skulle kunna hitta mer information där. Smuab alltså, Södra Munksjön Utvecklings AB.	
32	J	Är cybersäkerhet sett som en övergripande business risk, inom kommunen?	
33	O	Ja, jag sitter lite på fel nivå för att besvara på det tycker jag. Men min känsla är att ja, det måste vara en övergripande säkerhetsfråga	K&A-K
34	J	Har ni någon typ av cyber säkerhetspolicies eller projekt för att skapa medvetenhet och träna anställda inom detta?	
35	O	Det är väl lite si och så med det, det är möjligt att det finns, men man märker inte av det speciellt mycket. Det är många, många anställda i kommunen och de flesta handlar om mail och sådär. Det kan ibland vara ett problem att få folk att inte öppna spam mail och liknande. Jag kan säga att det, det finns ganska stora behov av att få folk att förstå	K&A O-P

		vad det är dom ska öppna och inte ska öppna och såna saker. Nivån är kanske inte så hög, inte heller kännedomen.	
36	G	Nä, precis. Vi kommer in här lite mer på finansiella faktorer som kan påverka cybersäkerhet. När det kommer just till cybersäkerhet, budgeterar ni specifikt för detta eller ingår det i IT-budget?	
37	O	Det var en bra fråga, det kan jag inte svara på faktiskt.	OI
38	J	Då kan vi fortsätta, upplever du att kostnaden är en faktor när man beaktar cybersäkerhet?	
39	O	Hittills har vi inte tagit upp det, men jag tror nästan att vi har förutsatt att den delen av, av det som gäller appar och liknande som vi vill utveckla, då ser vi det nog som att det är en del som ska ingå i arbetet, men sen vet jag inte om det de facto är så.	OI
40	J	Okej, anser du att tillräckligt mycket pengar spenderas på cybersäkerhet?	
41	O	Väldigt bra fråga, men jag har nog faktiskt inget svar där. Jag har dålig koll på den frågan helt allmänt så jag får avstå från att svara på den frågan.	OI
42	G	Du nämnde tidigare när att ni hade appar som tredje parter gjorde åt er, hur stor förtroende har ni för just, leverantörer eller kontraktörer gällande deras säkerhet?	
43	O	Ja, för, jag tror att vi förutsätter att IT säkerheten är bra, men sen har det visat sig i vissa sammanhang att det inte riktigt har varit så bra som vi har tänkt. Men då har vi, i de sammanhangen som vi har upptäckt detta, så har vi styrt så att det har gått i rätt riktningen.	OS-T

44	G	Jag kan tänka mig att det är mycket offentliga uppköp, i de avtalen finns det specifika klausuler som behandlar cybersäkerhet?	
45	O	Jag är osäker om det har gjorts tidigare men där kan man nog säga att, sannolikt så är det bättre nu än tidigare, medvetenheten om det här på IT-sidan och även bland oss som har ägnat oss åt viss upphandlingen och tjänster och så. Där har vi blivit mer medvetna idag än vad vi har varit tidigare.	
46	J	Bara för att gå tillbaka lite snabbt, så nämnde du att ni har hittat brister tidigare hos leverantörer, har du något exempel på vad det var eller om du kan utveckla det lite?	
47		Det är egentligen ganska basalt, det var en http adress istället för en https adress. Så det är ett exempel då, där fanns det, det fanns lite mer att hämta där. Det är inte jag som håller på med det specifikt men det är ett fall jag vet, och ja, det är ju tillräckligt för att åtgärda kan man ju säga.	OI
48	J	Ja absolut.	
49	G	Intressant. Det var i princip alla våra frågor.	

Appendix 5 – Interview 6

Sex: Female

Age: 30+

Alias: L

Date and Time: 2018-05-09, 13:06

Type of interview: Telephone interview

Duration: 37:01

L: Interviewee 6

G: Gustav Jansäter

J: Joel Olsson

#	Speaker		Code
1	J	So, do you experience that in smart city initiatives in your city, is there a sufficient focus and measures taken regarding cyber security?	
2	L	Yes, we have I think it’s 5 years ago, or 4 years ago, we - hackers accessed our open data portal and in 2014 we actually had an accident where some data was leaked which was personal. And after that we sat down and, security task force in the city that runs through every smart city initiative and has certain criteria that has to be fulfilled. So that’s a lot of attention to that.	OI
3	G	That’s very interesting actually.	
4	J	So that’s more of a general question so now we go into more specific questions I guess. So what possible risks of smart city initiatives do you see?	

5	L	Well, there are of course several and there is this dilemma between creating better services and not surveilling too much or having leaks in security. But we're not that mature in our smart city initiatives - I don't think they affect crucial infrastructure yet. At least, it hasn't been in discussion in terms of human lives but of course the GDPR is big here as well. And applied in all departments to make sure that we comply to that. We do some experiments with separating data from person, personal identifiers so we can aggregate data and use them without being able to link them to a certain person.	K&A-RA
6	G	Do you see that there is, as you mentioned before there was someone who leaked the data from an early initiative. Do you think there are any threats, external threats against smart city initiatives, as of now?	
7	L	I mean, the more services that we digitize the more vulnerable they get. But of course our health systems are more and more online but still in distributed systems. No, I don't think lives depend on it. But I think definitely, these years digitization of the core business of the city is starting. Until now smart city has been primarily pilot projects, lighting projects…	K&A-RA
8	J	Can you repeat that last part, because … our connection seems pretty bad right now. Let's see. What should we do?	
9	G	Not sure, can you hear us well?	
10	L	L: Yes.	
11	G	Because sometimes there is an interruption in the service.	
12	L	We can do it on the phone maybe?	

13	G	We can try a little bit more, but if it continues we can call you on the phone.	
14		//Phone call instead.	
15	L	Can you hear me?	
16	G	Yes! Can you hear us?	
17	L	Yes.	
18	J	So, let's just go back.	
19	G	Yes, do you follow any security standards in your smart city initiatives?	
20	L	Well, as I mentioned earlier we have this security task force - they have a set of written standards that they follow for all initiatives. I don't know them by heart, but I can send them to you.	O-OA
21	G	Ah. I'll try to mail you once transcription is done and you could maybe send them to me. If you have time, that is.	
22	L	Yes, sure. Maybe someday I will have time.	
23	G	Ok! Do you overarching, any encompassing cyber security strategy?	

24	L	No, we don’t have a strategy but I am sure there is a policy. That is for city digitalisation in general and not specifically for smart city initiatives. Many of the smart city initiatives are in collaboration with actors in the city like the university, companies and so on. Usually, if it affects our own systems it’s our own policy, of course, that rules. But sometimes it’s also the university and they use facilities in the city for example which is then another case.	O-BA
25	J	Ok. So I guess it’s generally the same security strategy as with all the projects in the city, there is nothing specific.	
26	L	Exactly.	
27	G	And there are a lot of cooperations between the different actors in regards to cyber security?	
28	L	Not to my knowledge. I know that on a governmental level there is a lot of collaboration between cities, regions and the national government. But maybe you should interview our head of security - of IT security, because this person will know a lot more.	
29	G	That’s fine, we think you’re absolutely the right person for this because we don’t want the exact knowledge about cyber security, just to know how much focus there is in the projects.	
30	L	Ok. That makes sense.	
31	J	Yeah. Do you conduct any risk analysis when considering smart city projects?	
32	L	It depends on the project. I mean, we run all our projects, not coordinated, project by project if it’s our own organisation, so we don't have a vote that decides what new projects should be put into the sea, it’s	

		not that systematic. So we start a new project, it will have it's own procedures and if it has something critical in terms of IT infrastructure it's within the city, there should be a risk analysis connected to it.	
33	G	Ok. When you think about the, because as you mentioned before, there were a lot of actors in the smart city initiatives, do you consider any security flaws when there are so many different actors and so many different systems? For the interoperability and interconnectedness, do you see any risks there - any security flaws?	
34	L	Probably. It hasn't been a big part of the agenda, yet. Usually it comes when you start to complete projects and set it up, and you have meetings and you discuss what kind of risks there might be but on a general level it hasn't been a very big part of the agenda. Yet! We haven't had any accidents since the big one in 2014. But I mean, sometimes it takes something like that for the attention on it to be sharpened, again. But we are not very mature on smart cities and we, we have lots of initiatives and we are also leading in some areas but in terms of digitalisation of the core business we are not very far, and I don't think anyone is but it is the next step for smart cities and it is also bigger risks, will occur.	K&A-RA
35	G	That is also something we found, there are not that many cities that are so in the future with smart city initiatives, they are in the beginning phase right now and there is a lot of focus on functionality. Is that the same for Aarhus as well, more focuses on functionality than cyber security?	
36	L	Yeah, good question. The focus is very much on what is the problem that we want to solve and then can technology be a solution or not? So, it's not so much that we have this technology, where can we apply it? It's more we have this challenge, can we solve it with technology.	K&A-NC
37	J	So, do you have any - do you have any employees that are working with cyber security in smart city initiatives?	

38	L	No. There are people all around on the city that works with cyber security - digitisation of the city. They would be used for smart city projects and can be included; we don't have any dedicated cyber security person.	O-OA
39	J	Ok.	
40	G	And that is the IT department in the city?	
41	L	Yes, I mean, we're organised in six different departments. They all have their own digitalisation units and then we have the mayor's department, which have the overall strategic digitalisation and so on. But it is decentralised.	O-OA
42	J	But do your smart city initiatives overarch these different departments?	
43	L	Yes, they do, depending on what project it is, we have had most of our projects in the technical department, with the city and transportation projects and so on. But also many in the citizen service department. Sometimes they collaborate, three or four departments in one project. Usually, there is one main driver that coordinates the others.	
44	G	I know you mentioned this before but, is cyber security consider when discussion new strategies or new projects?	
45	L	Yes, I mean. Once projects have been deicide and are going to be implemented, this usually occurs. The discussion comes up, and I guess that if we discuss a new project that has high risks connected to it we would probably would have had the discussion already. But I do not think we had any this far, but it has been a major concern for us. I would imagine that when we start our integration of our digital health systems, where the city has some the region has some, and the regions has hospitals and the cities have doctors and all of that. So once we connect this data on health, there will be some, discussions I guess since this will be very complicated so. That should be interesting in concern to security as well.	O-BA

46	J	So is cyber security seen as an overall business security issue for your city?	
47	L	Not really, no. I mean, some companies of course have it very high on their agenda because they need to. But it is not something that is a major issue for us.	K&A-NC
48	G	Are there any security policies or projects for creating user awareness of cyber security in the city?	
49	L	Yes, we have a bigger initiative called, digital trygghet. It's about feeling safe and secure, for instance when you buy and sell stuff online, it's about young people on the internet, it's about no sharing on the internet of pornografi, sharing naked pictures among school children, so there is lots of training programmes. We just had a huge conference for parents and children parallel. About how to behave on the internet and about understanding what children do online, where one should pay attention. There was this huges case this spring where 1200 teenagers was sued because they had shared a video of young people having sex. So it is a pretty big issue here.	
50	G	Do you have any projects within your organisation for increasing cyber security awareness?	
51	L	Yes, I mean, I’m not completely into the entire program but every time we hire a new person you have to watch security videos before you get started, so in the introduction of new employees, there is also a one hour course, in term of how to behave at the workplace. However, I have been here for some years, and there has not been any follow-up, so.	O-P
52	J	Has this kind of policies and training change after you implemented smart city initiatives?	

53	L	I think actually our leak on the open data portal did change the policies in the city, in terms of paying more attention to new projects and especially smart city projects and security.	OI
54	J	So, we are going into the financial questions about cyber security and the first question is, do you budget for cyber security in smart city projects?	
55	L	That is a good question, I mean, I have not been that concretely into these projects but I would imagine that we do, but I would have to check. I mean, if we do a type of traffic sensor data project I'm sure that, like I mentioned before it is all a part of the cities general standard for introduction new projects and digital security is part of that. And every new project has to go through this security taskforce so, it is not a complete question but if there's tension to it, or a big risk I am sure that there will be allocated resources to take care of that.	K&A
56	G	So, when cyber security has been introduced to a project, has cost ever been a factor that made you disregard cyber security?	
57	L	Actually, I am not able to answer that question, I do not know. But I do know that cyber security and security of public data is a very high priority. The trust that we have towards our citizens is extremely important and it is high on the agenda, so I do not think it would happen. If there was not enough money to secure it than I think the project would be discarded. That is, I can not guarantee it, but that would be my best guess.	F-CI
58	G	So do you feel like enough money is being spent on cyber security in smart city projects?	
59	L	I do not know, because I do not know what it costs in terms of. I'm not really into the details.	

60	G	So you mentioned before that there are a lot of actors within smart city projects. How much trust do you put on your suppliers and contractors on their security when they deliver services and products to you?	
61	L	That is very important, they have to live up to certain standards like two factor identification and things like that. So in order to deliver to the city, you have to live up to the city's security standard.	OS-C
62	G	Is this included in the contracts with your suppliers and vendors, is this in the contract?	
63	L	Yes, usually it is in the tender and it will be in there so you have to comply with this and this and this	
64	J	Who sets the requirements? Like who decides what is enough and not enough and so on.	
65	L	It would be the department that does the tender, but of course the overall digitisation policy is going to influence it, so it would be in the IT department and the relevant department to do it.	O-BA
66	J	Did the data leak incident affect the amount of emphasis you put on cyber security?	
67	L	Yes, and I think we were very lucky to have an incident very early.	
68	G	Do you think it would be as much focus on cyber security as there is today if there was no incident before?	
69	L	No, I do not think so, the taskforce was put down because of this incident. So of course it is the interest of cyber security and its dark sides of digitalisation has become more and more apparent to people. I have been running an event for five years now at internet week in Denmark	OI

		that focuses on digitalisation and this year there has been so much focus the negative sides of digitalisation, security leaks, you know the whole Facebook-Cambridge Analytica incident and so on, so it is a lot of attention to it. Already, three years ago we had a conference in cyber security and it was totally overbooked so it is something that both companies and municipalities and students are interested in.	

References

Al-Dairi, A. and Tawalbeh, L., (2017). Cyber Security Attacks on Smart Cities and Associted Mobile Technologies. Procedia Computer Science, 109C, pp. 1086-1091

Alhader, M., and Rodzi, A. (2009). The smart city infrastructure development & monitoring. *Theoretical and Empirical Researches in Urban Management*, *4*(2 (11), 87-94.

Alawadhi, S., Aldama-Nalda, A., Chourabi, H., Gil-Garcia, J. R., Leung, S., Mellouli, S., ... and Walker, S. (2012). Building understanding of smart city initiatives. In *Inter national Conference on Electronic Government* (pp. 40-53). Springer, Berlin, Heidelberg.

Baccarne, B., Mechant, P., & Schuurman, D. (2014). Empowered cities? An analysis of the structure and generated value of the smart city Ghent. In Smart City (pp. 157- 182). Springer, Cham.

Baig, Z., Szewcyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., Sansurooah, K., Syed, N. and Peacock, M., (2017). Fu ture challenges for smart cities: Cyber-security and digital forensics. Digital Investigation, 22, pp. 3-13

Bakıcı, T., Almirall, E., & Wareham, J. (2013). A smart city initiative: the case of Barcelona. *Journal of the Knowledge Economy*, *4*(2), 135-148.

Bartunek, J.M., Rynes, S.L. and Ireland, R.D., (2006). What makes management research interesting, and why does it matter? *Academy of management Journal*, *49*(1), pp.9-15.

Bartoli, A., Hernández-Serrano, J., Soriano, M., Dohler, M., Kountouris, A. and Barthel, D., (2011). Security and privacy in your smart city. In *Proceedings of the Barcelona smart cities congress* (Vol. 292).

Bhattacherjee, A., (2012). Social science research: Principles, methods, and practices.

Boison, G., Bohmayr, W., Deutscher, S. and Bechauf, M., (2017). It Takes a Coalition to Pro tect the Internet of Things. *BCG*

Bowles, J., (2018). [Online] America’s cities are under cyberattack. That’s bad news for IoT and Smart Cities. Available at: https://diginomica.com/2018/03/30/americas- cities-cyberattack-thats-bad-news-iot-smart-cities/ [Accessed: 17 May]

Bradbury, D., (2012). SCADA: a critical vulnerability. Computer Fraud and Security, Volume 2012, Issue 4, April 2012, Pages 11-14. http://www.sciencedirect.com/science/article/pii/S1361372312700301

Brenna, M., Falvo, M. C., Foiadelli, F., Martirano, L., Massaro, F., Poli, D., and Vaccaro, A. (2012). Challenges in energy systems for the smart-cities of the future. In Energy Conference and Exhibition (ENERGYCON), 2012 IEEE International (pp. 755-762). IEEE.

Breuer, J., Walravens, N., and Ballon, P. (2014). Beyond defining the smart city. Meeting top-down and bottom-up approaches in the middle. *Tema. Journal of Land Use, Mobility and Environment*.

Brinkmann, S., and Kvale, S. (2005). Confronting the ethics of qualitative research. *Journal of constructivist psychology*, *18*(2), 157-181.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I., (2010). Information security policy com pliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), pp.523-548.

Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. (2003). The economic cost of pub licly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431-448.

Caragliu, A., Del Bo, C., and Nijkamp, P. (2011). Smart cities in Europe. Journal of urban technology, 18(2), 65-82.

Carr, M., (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), pp.43-62.

Chabinsky, S. R. (2010). Cyber security strategy: A primer for policy makers and those on the front line. J. Nat'l Sec. L. & Pol'y, 4, 27.

Chakravorti, B. and Chaturvedi, R.S., (2017). [Online] Future Doesn't Look Like Science Fiction. Harvard Business Review. Available at: https://hbr.org/2017/10/the- smart-society-of-the-future-doesnt-look-like-science-fiction [Accessed: 22 February]

Chang, S., and Lin, C. S. (2007). Exploring organizational culture for information security man agement. *Industrial Management & Data Systems*, *107*(3), 438-458.

Check Point Research, (2017). [Online] A New IoT Botnet Storm is Coming. Check Point Re search. Available at: https://research.checkpoint.com [Accessed: 23 February]

Chen, R.S., Sun, C.M., Helms, M.M. and Jih, W.J.K., (2008). Aligning information techno logy and business strategy with a dynamic capabilities perspective: A longitudinal study of a Taiwanese Semiconductor Company. *International Journal of Information Management*, *28*(5), pp.366-378.

Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J.R., Mellouli, S., Nahon, K., Pardo, T.A. and Scholl, H.J., (2012). Understanding smart cities: An integrative framework. In *Sys tem Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 2289-2297). IEEE.

Cocchia, A., (2014). Smart and digital city: A systematic literature review. In *Smart city* (pp. 13-43). Springer, Cham.

Cooke, P. and De-Propris, L., (2011). A policy agenda for EU smart growth: the role of creative and cultural industries. Policy Studies, 32(4), pp.365-375.

Curry, E., Dustdar, S., Sheng, Q. Z., and Sheth, A., (2016). Smart cities–enabling services and ap plications. Journal of Internet Services and Applications, 7(1), 6.

Dameri, R. P. and Rosenthal-Sabroux, C., (2014). Smart City, Springer

Dell and Intel, (2016). Smart Cities Start with Smart Buildings. [Online] Harvard Business Re view. https://hbr.org/sponsored/2016/01/smart-cities-start-with-smart- buildings [Accessed: 22 February]

Doherty, N. F., Anastasakis, L., and Fulford, H., (2009). The information security policy un packed: A critical study of the content of university policies. *International Jour nal of Information Management*, *29*(6), 449-457.

Elmaghraby, A.S. and Losavio, M.M., (2014). Cyber security challenges in Smart Cities: Sa fety, security and privacy. Journal of advanced research, 5(4), pp.491-497.

Etzkowitz, H., and Leydesdorff, L., (2000). The dynamics of innovation: from National Systems and "Mode 2" to a Triple Helix of university–industry–government relations. *Re search policy*, *29*(2), 109-123.

European Commision Strategic Energy Technologies Information Systems. (n.d.) [Online] Avai lable at:https://setis.ec.europa.eu/set-plan-implementation/technology- road maps/european-initiative-smart-cities Accessed: 25 March] European Commision Innovation and Networks Executive Agency. (n.d.) [Online] Available at: https://ec.europa.eu/inea/en/horizon-2020/smart-cities-communities [Acces sed: 25 March]

European Commision Innovation and Networks Executive Agency. (n.d.) [Online] Available at: https://ec.europa.eu/inea/en/horizon-2020/smart-cities-communities [Acces sed: 25 March]

EU-Gugle. (n.d.) [Online] Project description. Available at: http://eu-gugle.eu/project/ [Ac cessed: 13 March]

EY, (2016). [Online] Cyber Security A necessary pillar of Smart Cities. Available at: http://www.ey.com/Publication/vwLUAssets/ey-cyber-security-a-necessary- pillar-of-smart-cities/$FILE/ey-cyber-security-a-necessary-pillar-of-smart- cities.pdf [Ac cessed 24 February]

Fereday, J., and Muir-Cochrane, E., (2006). Demonstrating rigor using thematic analysis: A hy brid approach of inductive and deductive coding and theme development. *Interna tional journal of qualitative methods*, *5*(1), 80-92.

Ferraz, F.S. and Ferraz, C.A., (2014). Smart City Security Issues: Depicting Information Security Issues in the Role of an Urban Environment. IEEE/ACM 7th Internat ional Confer ence on Utility and Cloud Computing, London, pp. 842-847.

Ferrer, J. N., Costa, S., Chira, C., Deambrogio, E., Horatz, M., Lindholm, P., Nielsen, D., Pa sic, E., and Bhana, R., (2013). Using EU funding mechanisms for smart cities, in *Smart Cities and communities, ed., Smart Cities stakeholder platform.*

Finkle, J., (2017). [Online] U.S. warns public about attacks on energy, industrial firms. *Reu ters*. Available at: http://www.reuters.com [Accessed: 22 February]

Goles, T., White, G. B., and Dietrich, G., (2005). Dark screen: An exercise in cyber security. *MIS Quarterly Executive*, *4*(2), 303-318.

Gold, S., (2009). The SCADA challenge: securing critical infrastructure. Network Security, Vol ume 2009, Issue 8, August 2009, Pages 18-20. http://www.sciencedirect.com/sci ence/article/pii/S1353485809700789

Gonzalez, J. J., (2005). Towards a cyber security reporting system–a quality improvement pro cess. In *International Conference on Computer Safety, Reliability, and Secu rity* (pp. 368-380). Springer, Berlin, Heidelberg.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R., (2005). 2005 CSI/FBI com puter crime and security survey. *Computer Security Journal*, *21*(3), 1. Gummesson, E., (2003). All research is interpretive! *Journal of business & indus trial marketing*, *18*(6/7), 482-492.

Hall, R.E., Bowerman, B., Braverman, J., Taylor, J., Todosow, H. and Von Wimmersperg, U., (2000). *The vision of a smart city* (No. BNL--67902; 04042). Brookhaven Nat ional Lab., Upton, NY (US).

Harrison, C., Eckman, B., Hamilton, R., Hartswick, P., Kalagnanam, J., Paraszczak, J. and Wil liams, P., (2010). Foundations for smarter cities. *IBM Journal of Research and De velopment*, *54*(4), pp.1-16.

Henderson, J. C., & Venkatraman, H. (1993). Strategic alignment: Leveraging information tech nology for transforming organizations. *IBM systems journal*, *32*(1), 472- 484.

Hevner, A., and Chatterjee, S., (2010). *Design research in information systems: theory and prac tice* (Vol. 22). Springer Science & Business Media.

Heo, T., Kim, K., Kim, H., Lee, C., Ryu, J.H., Leem, Y.T., Jun, J.A., Pyo, C., Yoo, S.M. and Ko, J., (2014). Escaping from ancient Rome! Applications and challenges for designing smart cities. In *Transactions on Emerging Telecommunications Technologies,* 25(1), pp.109-119.

Hollands, R. G., (2008). Will the real smart city please stand up? Intelligent, progressive or entre preneurial?. *City*, *12*(3), 303-320. Igure, V. M., Laughter, S. A., and Williams, R. D. (2006). Security issues in SCADA networks. Computers & Security, 25(7), 498-506.

Igure, V. M., Laughter, S. A., and Williams, R. D. (2006). Security issues in SCADA networks. Computers & Security, 25(7), 498-506.

International Telecommunications Union (ITU), (n.d.). ITU-TX.1205: series X: Data networks, open system communications and security: telecommunication security: Overview of Cyber security 2008

Jin, J., Gubbi, S. Marusic and Palaniswami, M., (2014). An Information Framework for Creating a Smart City Through Internet of Things. IEEE Internet of Things Journal, vol. 1, no. 2, pp. 112-121, April 2014.

John-Green, M. S., and Watson, T., (2014). Safety and Security of the Smart City-when our infra structure goes online.

Johnston, A. C., and Hale, R., (2009). Improved security through information security governance. Communications of the ACM, 52(1), 126–129.

Kannan, K., Rees, J., and Sridhar, S., (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce* (12:1), Fall 2007, pp 69-91.

Kayworth, T., & Whitten, D., (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*, Vol. 9 No. 3 / Sep 2010 Khalfan, A. M., (2004). Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. *International Journal of Information Management*, *24*(1), 29-42.

Khan, R., Khan, S. U., Zaheer, R., and Khan, S., (2012). Future internet: the internet of things ar chitecture, possible applications and key challenges. In *Frontiers of Information Technology (FIT), 2012 10th International Conference on* (pp. 257-260). IEEE.

Khatoun, R., and Zeadally, S., (2016). Smart cities: concepts, architectures, research opportunities. *Communications of the ACM*, *59*(8), 46-57.

Kitchin, R., (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, *79*(1), pp.1-14.

Klinpratum, T., Saivichit, C., Elmangoush, A. and Magedanz, T., (2014). Toward Inter connecting M2M/IoT Standards: Interworking Proxy for IEEE1888 Standard at ETSI M2M Platforms. In *29th International Technical Conference on Cir cuit/Systems Computers and Communications (ITC-CSCC 2014)* (pp. 763-766).

Knapp, K. J., Marshall, T. E., Rainer Jr, R. K., and Morrow, D. W., (2006). The top informat ion security issues facing organizations: What can government do to help. *Network se curity*, *1*, 327.

Krefting, L., (1991). Rigor in qualitative research: The assessment of trustworthiness. *American journal of occupational therapy*, *45*(3), 214-222.

Kuilboer, J.P. and Ashrafi, N., (2016). Internet of Things: A Security Challenge. AMCIS 2016 Proceedings. http://aisel.aisnet.org/amcis2016/TREO/Presentations/41/

Kuypers, M. A., Maillart, T., and Pate-Cornell, E., (2016). An empirical analysis of cyber security Incidents at a large organization. *Department of Management Science and Engineering, Stanford University, School of Information, UC Berkeley*

Kvale, S., (2006). Dominance through interviews and dialogues. *Qualitative inquiry*, *12*(3), pp.480-500.

Kyriazis, D., Varvarigou, T., White, D., Rossi, A., and Cooper, J., (2013). Sustainable smart city IoT applications: Heat and electricity management & Eco-conscious cruise control for public transportation. World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Works hops on a (pp. 1-5). IEEE.

Kwon, J., Ulmer, J. R., and Wang, T., (2012). The association between top management *in* volve ment and compensation and information security breaches. *Journal of In formation Systems*, 27(1), 219–236.

LaBuda, R.J. and Gillespie, M.H., (2017). The Internet of Things: Current Issues and Future Prob lems. SAIS 2017 Proceedings. 24. https://aisel.aisnet.org/sais2017/24

Leydesdorff, L. and Deakin, M., (2013). The triple helix model of smart cities: a neo- evolution ary perspective. In Smart Cities (pp. 146-161). Routledge.

Legezo, D., (2016). [Online] How to trick traffic sensors. AO Kaspersky Lab. Available at: https://securelist.com/how-to-trick-traffic-sensors/74454/ [Accessed: 23 March]

Ma, Q., Schmidt, M.B. and Pearson, J.M., (2009). An integrated framework for information secu rity management. *Review of Business*, *30*(1), p.58.

Manville, C., Cochrane, G., Cave, J., Millard, J., Pederson, J. K., Thaarup, R. K., ... and Kotterink, B., (2014). Mapping smart cities in the EU. *Policy Department – Econo mic and Scientific Policy. European Parliament.*

Marsal-Llacuna, M. L., Colomer-Llinàs, J., and Meléndez-Frigola, J., (2015). Lessons in ur ban monitoring taken from sustainable and livable cities to better address the Smart Cities initiative. Technological Forecasting and Social Change, 90, 611- 622.

McFadzean, E., Ezingeard, J.N. and Birchall, D., (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. Online Information Review, 31(5), pp.622-660.

Mitton, N., Papavassiliou, S., Puliafito, A., and Trivedi, K. S., (2012). Combining Cloud and sensors in a smart city environment.

Munro, K., (2008). SCADA – A critical situation. *Network Security*. February 2008, Issue 1, pp. 4-6.https://ac.els-cdn.com/S1353485808700059/1-s2.0- S1353485808700059-main.pdf?_tid=92eb52d0-b8d5-11e7-aa61- 00000aab0f02&acdnat=1508861489_cc700dcc0b5a9b778cc46335238bce95

Nam, T. and Pardo, T.A., (2011). Conceptualizing smart city with dimensions of technology, people, and institutions. In *Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times* (pp. 282-291). ACM.

Negre, E., Rosenthal-Sabroux, C., & Gascó-Hernández, M. (2017, January). Introduction to Smart Cities, Smart Government, and Smart Governance Minitrack. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Oehme, R., (2017). [Online] Det krävs krafttag för att stärka cybersäkerheten i samhället. Ny Teknik. Available at: https://www.nyteknik.se/opinion/det-kravs-krafttag-for- att-starka-cybersakerheten-i-samhallet-6820192 [Accessed 21 February]

Orlikowski, W. J., and Baroudi, J. J., (1991). Studying information technology in organizations: Research approaches and assumptions. *Information systems research*, *2*(1), 1-28.

Papa, R., Gargiulo, C., and Galderisi, A., (2013). Towards an urban planners' perspective on smart city. *TeMA Journal of Land Use, Mobility and Environment*, 6 (01), (pp 5 - 17).

Pearlson, K. E. and Saunders, C. S., (2009). Managing and Using Information Systems. NY: Wiley. Petrolo, R., Loscri, V., and Mitton, N., (2014). Towards a smart city based on cloud of things. In *Proceedings of the 2014 ACM international workshop on Wireless and mobile technologies for smart cities* (pp. 61-66). ACM.

Petrolo, R., Loscri, V., and Mitton, N., (2014). Towards a smart city based on cloud of things. In *Proceedings of the 2014 ACM international workshop on Wireless and mo bile technologies for smart cities* (pp. 61-66). ACM.

Pierce, P., and Andersson, B., (2017). Challenges with smart cities initiatives–A municipal decision makers' perspective. *Proceedings of The Hawaii International Conference on System Sciences.* Institute of Electrical and Electronics Engineers Inc., s. 2804-2813 10 s.

Pierce, P., Ricciardi, F. and Zardini, A., (2017). Smart Cities as Organizational Fields: A Framework for Mapping Sustainability-Enabling Configurations

Plachinkova, M., Vo, A. and Alluhaidan, A., (2016). Emerging Trends in Smart Home Secu rity, Privacy, and Digital Forensics. 22nd Americas Conference on Information Systems, San Diego. http://aisel.aisnet.org/amcis2016/ITProj/Presentations/23/

Potoczny-Jones, I., (2015). [Online] IoT Security & Privacy: Reducing Vulnerabilities. Network Computing. Available at: https://www.networkcomputing.com/internet-things/iot-security-privacy- reducing-vulnerabilities/807681850 [Accessed 21 February]

Puhakainen, P., and Siponen, M., (2010). Improving employees' compliance through inform ation systems security training: an action research study. *Mis Quarterly*, 757- 778.

Pötsch, T., Marwat, S. N. K. K., Zaki, Y., and Gorg, C., (2013). Influence of future M2M commu nication on the LTE system. In *Wireless and Mobile Networking Confer ence (WMNC), 2013 6th Joint IFIP* (pp. 1-4). IEEE.

Recker, J., (2012). *Scientific research in information systems: a beginner's guide*. Springer Sci ence & Business Media.

Rowe, B. R., and Gallaher, M. P., (2006). Private sector cyber security investment strategies: An empirical analysis. In *The fifth workshop on the economics of information security (WEIS06)*.

Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M. and Oliveira, A., (2011). Smart cities and the future internet: Towards cooperation frameworks for open innovation. In *The future internet assembly* (pp. 431-446). Springer, Berlin, Heidelberg.

Singh, A.N., Picot, A., Kranz, J., Gupta, M.P. and Ojha, A., (2013). Information security manage ment (ism) practices: Lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management*, *14*(4), pp.225-239.

Siponen, M., Mahmood, M. A., & Pahnila, S., (2009). Technical opinion: Are employees put ting your company at risk by not following information security policies?. *Communications of the ACM*, *52*(12), 145-147.

von Solms, B. and von Solms, R., (2005). From information security to… business security?. *Computers & Security*, *24*(4), pp.271-273.

von Solms, R. and van Niekerk, J., 2013. From information security to cyber security. *Comp ters & security*, *38*, pp.97-102.

Sommestad, T., Ekstedt, M., and Holm, H. (2013). The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. *IEEE Systems Journal*, *7*(3), 363-373.

Soomro, Z.A., Shah, M.H. and Ahmed, J., (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Man agement*, *36*(2), pp.215-225.

Step Up Europe. (n.d.) [Online] Project description. Available at: https://www.stepupsmartci ties.eu/ [Accessed: 13 March] Strauss, A., and Corbin, J. M. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Sage Publications, Inc.

Strauss, A., and Corbin, J. M. (1990). *Basics of qualitative research: Grounded theory proce dures and techniques*. Sage Publications, Inc.

Stuckey, H. L., (2015). The second step in data analysis: Coding qualitative research data. *Journal of Social Health and Diabetes*, 3(1), 7.

Sveen, F. O., Torres, J. M., and Sarriegi, J. M., (2009). Blind information security strategy. *Inter national Journal of critical infrastructure protection*, *2*(3), 95-109.

Syed, D., Chang,T.H., Svetinovic, D., Rahwan, T., and Aung, Z., (2017). Security for Com plex Cyber-Physical and Industrial Control Systems: Current Trends, Limitat ions, and Challenges. PACIS 2017 Proceedings. 180. https://aisel.aisnet.org/pacis2017/180

Thibodeaux, T., (2017). [Online] Smart Cities Are Going to Be a Security Nightmare. Har vard Business Review. Available at: https://hbr.org/2017/04/smart-cities-are- going-to-be-a-security- nightmare [Accessed 23 February]

Townsend, A. M., (2013). Smart cities: Big data, civic hackers, and the quest for a new utopia. WW Norton & Company.

Vilajosana, I., Llosa, J., Martinez, B., Domingo-Prieto, M., Angles, A., and Vilajosana, X., (2013). Bootstrapping smart cities through a self-sustainable model based on big data flows. *IEEE Communications magazine*, *51*(6), 128-134.

Vlacheas, P., Giaffreda, R., Stavroulaki, V., Kelaidonis, D., Foteinos, V., Poulios, G., ... and Moessner, K., (2013). Enabling smart cities through a cognitive management frame work for the internet of things. IEEE communications magazine, 51(6), 102-111.

Walsham, G., (2006). Doing interpretive research. *European journal of information systems*, *15*(3), 320-330.

Wang, P., Ali, A. and Kelly, W., (2015). Data security and threat modeling for smart city infrastructure. In *Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on*(pp. 1-6). IEEE.

Washburn, D., Sindhu, U., Balaouras, S., Dines, R. A., Hayes, N., and Nelson, L. E., (2010). Helping CIOs understand “smart city” initiatives. *Growth*, *17*(2), 1-17.

Wenge, R., Zhang, X., Dave, C., Chao, L., and Hao, S., (2014). Smart city architecture: A tech nology guide for implementation and design challenges. *China Communications*, *11*(3), 56-69.

Williams-Grut, O., (2018). [Online] Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank. Available at: http://www.busi nessinsider.com/hackers-stole-a-casinos-database-through-a- thermometer-in-the-lobby-fish-tank-2018-4?r=US&IR=T&IR=T [Accessed: 27 May]

Yadav, P., Hasan, S., Ojo, A. and Curry, E., (2017). The Role of Open Data in Driving Sustainable Mobility in Nine Smart Cities.

Yar, M. (2006). Cybercrime and the internet: an introduction. In *Cybercrime and society* (pp. 1-20). London: SAGE Publications Ltd doi: 10.4135/9781446212196.n1

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things journal*, *1*(1), 22-32.

Zetter, K., (2011). [Online] H(ackers)2O: Attack on city water station destroys pump. WIRED. Available at: https://www.wired.com/2011/11/hackers-destroy-water- pump/ [Ac cessed: 25 March]