Risks and benefits of IoT appliances used in household and business environment

Toni Hakala

2019 Laurea

Laurea University of Applied Sciences

Risks and benefits of IoT appliances used in household and business environment

Toni Hakala
Security Management
Bachelor’s Thesis
November, 2019

Laurea University of Applied Sciences
Degree Programme in Security Management
Bachelor's Thesis

Abstract

Toni Hakala

Risk and benefits of IoT appliances in household and business environment

2019 Pages 30

The objective of this thesis is to raise the readers awareness about IoT technology and illustrate the risks and benefits it brings to the society. What makes this technology truly worthwhile despite the risks, has to be explored. IoT as a topic is exceedingly large since it is related to literally everything that surrounds us. This thesis concentrates into one area, which is appliances that utilize an internet connection to operate. Some of these appliances are used in a business environment as well, which is also considered in this thesis.

Knowledge base is gathered mostly from electronic sources and they are the main source of information for this thesis. The available information about IoT appliances from printed sources is still scarce, therefore articles and already conducted interviews or surveys are used as reliable sources to gather knowledge. This thesis uses qualitative methods for research and analysis. Interviews privately and via e-mail were conducted as a research method and gathered results were analysed using thematic analysis and inductive reasoning. A professional working in an IoT company and an appliance retailer were interviewed about their knowledge and opinions to gather overall understanding of people concerning IoT technology.

Despite the threats IoT home appliances have, the benefits for companies and consumers generally exceed the risks. The benefits vary depending on the use of an IoT appliance, which means that some appliances have greater benefits than others. Businesses benefit from IoT differently than households, but its effect in the end is the same for both parties. Utilizing IoT technology is cost-effective and it speeds up activities in business and home environment. In other words, it saves time and money.

The main security threat concerning IoT appliances, in most cases, is the user of the appliance. The negligence of people and ignorance about home network security causes unnecessary vulnerabilities, which could be prevented by spreading the knowledge about the importance of securing these home appliances. In addition, due to rapid development of technology especially the legislation is lagging behind, and this allows manufacturing of poorly secured appliances. Manufacturing appliances with proper network security costs more and it encourages certain companies not to invest in these security features. Therefore, consumers have to be careful while buying these appliances since they might contain a significant security risk. Nevertheless, these appliances which are utilized in home- and business environment are becoming more useful and common in the future.

Keywords: IoT, Security, Company, Home, Appliance

Laurea University of Applied Sciences **Tiivistelmä**
Degree Programme in Security Management
Opinnäytetyö

Toni Hakala

IoT kodinkoneiden käyttämisen riskit ja hyödyt koti- sekä työympäristössä

2019 Sivumäärä 30

Tämän opinnäytetyön tarkoituksena on lisätä lukijan tietoisuutta IoT teknologiasta ja siihen liittyvistä hyödyistä ja haitoista, joita se tuo yhteiskunnalle. Täytyy myös selvittää mikä tekee tästä teknologiasta käyttämisen arvoisen siihen kohdistuvista riskeistä huolimatta. IoT aiheena on erittäin laaja, koska se liittyy kaikkeen mikä meitä ympäröi. Tämä opinnäytetyö keskittyy yhteen tiettyyn alueeseen eli kodinkoneisiin, joilla on kyky hyödyntää internetyhteyttä toimiakseen. Joitain näistä kodinkoneista hyödynnetään myös yritys maailmassa, joten sekin huomioidaan tässä opinnäytetyössä.

Tämän opinnäytetyön tietämyskanta on kerätty suurimmaksi osaksi verkkolähteistä. Painetuista kirjoista saatava tieto on vielä vähäistä, joten siksi verkosta löytyviä artikkeleita ja jo tehtyjä haastatteluja tai kyselyitä on käytetty tiedon keräämisessä. Tässä opinnäytetyössä on käytetty laadullisia tutkimismenetelmiä tiedon keruussa ja sen analysoinnissa. Tutkimusmenetelmänä käytettiin haastattelua yksityisesti sekä sähköpostin välityksellä ja niiden tulokset analysoitiin käyttämällä teemoittelua sekä induktiota. IoT alalla työskentelevää ammattilaista sekä elektronisten laitteiden jälleenmyyjää haastateltiin, jotta heidän kokonaiskäsityksensä ja mielipiteet liittyen IoT teknologiaan voitiin selvittää.

Tietyistä IoT laitteissa sisältyvistä uhkista huolimatta aiheutuvat hyödyt yrityksille sekä kuluttajille yleisesti ylittävät haitat. Hyödyt vaihtelevat laitteen käyttötarkoituksen mukaan, joka tarkoittaa sitä, että joillakin laitteilla on enemmän hyötykäyttöä kuin toisilla. Yritykset hyötyvät IoT teknologiasta eri tavalla kuin kotitaloudet, mutta vaikutukset ovat molemmille osapuolille samat. IoT teknologian hyödyntäminen on kustannustehokasta ja se nopeuttaa toimintoja yrityksissä sekä kotitalouksissa. Toisin sanoen se säästää aikaa ja rahaa.

Suurin turvallisuusriski, joka kohdistuu IoT kodinkoneisiin useammissa tapauksissa on niiden käyttäjä. Ihmisten välinpitämättömyys sekä tietämättömyys kodin verkon turvaamisesta aiheuttaa tarpeettomia haavoittuvuuksia, jotka voitaisiin estää jakamalla tietoa paremmin älykkäiden kodinkoneiden turvaamisen tärkeydestä. Lisäksi teknologian ripeän kehittymisen takia erityisesti lainsäädäntö ei pysy perässä, joka mahdollistaa huonosti turvattujen laitteiden valmistamisen. Kunnon tietoturva ominaisuuksilla varustettujen kodinkoneiden valmistaminen maksaa enemmän, mikä kannustaa tiettyjä yhtiöitä olemaan sijoittamatta tietoturva ominaisuuksiin. Siksi kuluttajien täytyy olla varovaisia ja tarkkoja siitä minkälaisia kodinkoneita he ostavat, sillä niissä saattaa piillä vakavia tietoturvariskejä. Siitä huolimatta koti- ja työympäristössä käytettävät IoT kodinkoneet kehittyvät koko ajan ja niiden hyötykäyttö yleistyy tulevaisuudessa.

Avainsanat: IoT, Turvallisuus, Yritys, Koti, Älylaite

Table of Contents

1 Introduction

The early 20th century was the age of second industrial revolution. The introduction of steel, electricity and chemicals made the mass production of goods possible and easier. Moving became faster after locomotives, automobiles and bicycles made long distance traveling effortless. This aided households across the world when they were no longer dependent on self-made goods and machines (Niiler 2019). Many inventions were developed further, and new ones were created. Large number of these products facilitated the lives of people and helped society in countless ways. Among other things household appliances were these inventions which were created to improve living standards of an individual. Kerrigan (2018) states that without these appliances, which have been developed for centuries by professionals from different industries, kitchens would be less safe and inefficient.

Now electrically powered home appliances have been around over hundred years and they are daily present in our modern society. We take them for granted and many could struggle living without them. Life would still be inefficient and basic chores would simply be more time consuming, while preserving groceries would be extremely challenging. Nowadays home appliances are not the only devices that run with electricity. The spectrum of electronic home appliances has grown continually. Especially manufacturing of smart appliances has increased and companies are constantly competing to create more desirable and appealing products for consumers. Making home appliances more economical and controlling them remotely has been the trendsetter lately, while also allowing them to become more and more independent when connected to the internet.

Various appliance manufacturers have entered the Internet of Things or briefly IoT market to get their share from the business bringing their own design ideas with them. There are varying statements and statistics from different sources but according to cybersecurity company F-Secure (No date), there will be over 30 to 50 billion internet-connected devices by year 2020. This includes smart phones, televisions and computers as well. Everything everywhere is becoming without intermission connected and closer together.

There are countless articles and studies discussing about the alarming security threats of IoT technology. According to cybersecurity companies such as F-secure and Darktrace the security of IoT is insufficient especially in household appliances. IoT is somewhat new technology to be applied into household appliances. This causes new problems and releasing it to the market without decent safety measures cause unnecessary headache and risks for its users. Companies are so occupied competing with their competitors that, while they develop smart appliances, they usually disregard the security features. There have been several cases in the past where a home network was cyberattacked via an appliance and it can still occur today.

Consumers and companies are under frequent attacks and they might become even more common if cybersecurity and legislation does not keep up. It is up to the individual consumers and information security companies to fight against this modern threat.

This thesis aims to find out the reason behind vulnerabilities IoT appliances contain and evaluate the viability of IoT technology for homes and businesses. Two research questions define the main objective of this thesis. Do the benefits of IoT technology exceed the disadvantages? Do these IoT appliances have reasonable cause to be connected to the internet? In addition, finding the reason why it is incentive to develop this kind of technology for everything that surround us, despite the transparent risks needs to be clarified.

2 Influence of IoT

This section includes an explanation about the IoT and the theory behind its risks and benefits. In order to widen the perspective, a literature review was conducted. “The meaning behind literature review is to display different perspectives and show how the subject has been researched before, and how the ongoing research is related to the existing researches” (Hirsjärvi, Remes & Sajavaara 1997, 121). Information concerning IoT was gathered mostly from electronic sources, but printed sources were also used. Used literature about IoT for this thesis was mostly related to the whole field rather than exclusively to home appliances, which is not the scale of this thesis.

As we now know IoT is a short term for the internet of things, but what does it mean? How is it different from smart devices? Gilchrist (2017) states that there are a variety of explanations about IoT and its true meaning. Unfortunately, there is no clear definition of what it is, and it can cause confusion among people. “If we cannot agree on a definition then how can we secure it?” (Gilchrist 2017, 5). Many argue about the true definition, but there are few reasonable explanations on what it is and the way it differentiates from smart devices. Kevin Ashton is considered as the inventor of the term IoT and he sees the “connection to humanity as the distinguishing factor” (Smith 2017, 4). He means by this that computers and internet require a human to relay information, but this interaction is no longer required when IoT sensors can relay that information automatically and independently.

There are already a few household appliances and many smaller devices in the market that include IoT technology. Refrigerators, ovens, vacuum cleaners, televisions and speakers are among the first appliances to utilize this technology. “Almost half of internet-wired households have some sort of smart home device, with thermostats, smart home systems and smart appliances topping the list and the global smart home market is predicted to be worth $97.61 billion by 2025” (Tompkins 2017). And this prediction includes only the internal market of the

United States of America. From a global perspective it is becoming more and more appealing and profitable business.

In addition to appliances, there are more far-reaching implications that the IoT technology is capable of. “A thing, in IoT, can be physical objects like a bridge, a building, or a transport having sensors like vibration, temperature, and accelerometer, respectively, or human beings like a person wearing a smart watch or having a biochip implant; in IoT, all of them can have an IP address through which the sensor data can be transferred over a network” (Pal & Purushothaman 2017, 15). IoT can be spread to effect everything which surrounds us, and in the future, it has the capability to connect everything closer together. It is a respectable ambition, but it has its own challenges. Gilchrist (2017) states that though this vision is admirable, it is difficult to carry out. Reason behind this according to him is “due to a lack of standards and dominant technologies” (Gilchrist 2017, 24). This fact is also accepted by Pal and Purushothaman (2017) who explain that the standards are non-existent with IoT authentication and authorization.

Since there are no clear rules or laws in manufacturing, everyone can produce IoT devices in their own standards. To put it simply a device manufactured by Bosch is not able to communicate with a LG´s device, due to the fact that, although in the same network, they do not speak the same language. This brings many challenges observing from a security and privacy aspect, because technically diverse devices made by various manufacturers operate differently. Fortunately, there are international standards that help to guideline the manufacturing of IoT devices and these standards date back to 2017. However, problem with international standards is that using them is not compulsory. “Adoption of IEC standards by any country, whether it is a member of the Commission or not, is entirely voluntary” (International Electrotechnical Commission No date).

2.1 Threats for households

Since controlling devices remotely has been a growing trend, manufacturers have been steadily increasing the production volume of smart devices in the market. Making a large quantity of smart devices unfortunately comes with a downside. “Devices aimed at the home market tend to be inexpensive, as they still compete with their traditional, unconnected counterparts for the consumers' money. Manufacturers don't invest in security simply because they can't afford to do so and still maintain low prices. As a result, there is an increasingly large supply of poorly protected devices out there” (F-Secure No date).

In an interview conducted by MTV Uutiset (2018) a professional hacker Benjamin Särkkä agrees with this fact. According to him cheap IoT appliances, often if not always, lack the support of the manufacturer. These devices are connected to the home network but are not updated frequently enough or cannot be updated at all. There is no possibility to update these devices, because there is no clear way to do this. Gilchrist also supports this fact by stating that “a major issue with IoT devices was that those found to be faulty could not be updated over the Internet” (Gilchrist 2017, 132).

Reason behind this is simply in the viability of the service. Cheap smart devices are not profitable to maintain after their installation. This brings an increasing demand for information security companies to create reasonable solutions to strengthen the security of internet-connected devices, since the manufacturers of these risky devices are not keen to do that themselves. Consumer is often unaware about the security risks a bought IoT device may contain. As a matter of a fact, a consumer is not usually interested about the security features of the desired device in the first place. In the same interview conducted by MTV Uutiset (2018) F-Secure’s director of research Mikko Hyppönen stated that consumers most important argument while buying a new smart device is the cost and the color of it. When consumers buy this device, no one asks what kind of firewall the device has or ask about its safety features. Companies, therefore, will not invest into the safety features, because it would simply raise the price and it would undoubtedly reduce the number of paying customers.

Therefore, there are information technology companies developing user-friendly solutions to strengthen households and businesses information security. To name a few companies, F-Secure and Avast are ones to offer hardware that secure every connected device in the same network connection, without any extra effort. F-Secure has developed a security router which protects every device connected to the home network after installation and aspire to keep them all up to date (F-Secure No date). Avast on the other hand offers similar solution. They have developed hardware that can be implemented to an existing home network. It utilizes artificial intelligence to scan and detect suspicious behavior in “routers, PCs, mobile and IoT devices connected to users’ network”. After the scan it “provides solutions on how to fix issues found”. It even has an “improved device identification and more thorough detection of security vulnerabilities and similar weaknesses” which considerably improves users’ cybersecurity (Avast 2018).

Due to low efforts of smart appliance manufacturers, IoT has been suffering from a lack of credibility. There are cases that involve a home device which is used to gain access to the personal information of the victim. IT security company named Check Point Software Technologies Ltd revealed in October 2017 that they discovered a serious vulnerability in LG’s smart home infrastructure. LG’s own smartphone application called SmartThinQ had a weakness which the exploited. They made a fake account and were able to fool the system to take control of the real account. After exploiting the vulnerability, they were able to command every

IoT appliance which were in the same connection. They explain further in their article why it was a serious problem: “This vulnerability highlights the potential for smart home devices to be exploited, either to spy on home owners and users and steal data, or to use those devices as a staging post for further attacks, such as spamming, denial of service (as we saw with the giant Mirai botnet in 2016) or spreading malware” (Check Point 2017).

Mirai botnet was specifically designed to utilize unprotected IoT devices. A botnet requires computers with internet connection which are then controlled remotely by a hacker with a certain objective. These abused computers are poorly protected by their users and after they are exposed, they are in a hacker’s disposal in any way possible. It is harder to track down the source of a hack, when many innocent computers are used as a middleman. Same idea is adapted with modern IoT devices. These devices have enough performance to execute the same objective. Problem with these IoT home devices is that they have “no built-in ability to be patched remotely and are in physically remote or inaccessible locations” (Fruhlinger 2018).

Fortunately, there are cybersecurity companies like Check Point whose purpose is to both hack and identify these kinds of vulnerabilities, as well as reporting them back to the manufacturer. After finding these vulnerabilities in the vacuum cleaner, Check Point reported the findings to LG and the weakness in the system were quickly patched. Later all LG product users were able to update their application, which fixed the issue (Check Point 2017). This was just one case of insufficient security features concerning IoT. Sometimes, there is no security company to find these kinds of weaknesses, but instead hackers are the ones to exploit them. When that happens, it predisposes the victim to serious privacy issues. Since IoT appliances utilize cameras, microphones, sensors or all of them at the same time to gather data, they become attractive targets for hackers seeking financial benefit. Like in the Check Point´s HomeHack case, accessing a camera feed via vacuum cleaner to find out, if anyone is present in the building, then utilizing that information to break in and enter an empty building.

After one household device is compromised, every other device connected to the same home network is in disposal of an internet criminal. According to the CEO of F-Secure Samu Konttinen any kind of IoT device can be the weakest link in home environment. Mainly these devices are used as a tool to steal identities and make money from it. And if there are many of these devices together, they can be harnessed to perform a distributed denial of service attack or in short DDOS. Owners of the devices usually notices that their device has been used in DDOS attack, when the internet service is cut off by their operator (Uusitalo 2019). The damage can be even more dramatic, if the home computer or smart phone is connected to the same network as the other household devices. An outsider accessing the information contained in the computer such as e-mail and other credentials can have serious consequences.

Since manufacturers do not invest in network security of an appliance, especially if the appliance is cheap to make, it seems like the responsibility of securing them is in the hands of a consumer. In an article written by Banks (2018) the consumers behavior with IoT technology is not praiseworthy. He calls it “Plug and Play” culture when referring to the habit of consumers just installing an IoT device and leaving it be. It also does not help that people usually “re-use passwords, leave default passwords to routers, fail to update firmware on devices ranging from routers to smart TVs, and fail to deploy updates” (Banks 2018). He also claims that additionally with the lack of people’s interest to secure their devices, it is not clear for consumers if they are responsible to secure their devices. And when something happens it is easy for companies to blame consumers for their poor network security due to lack of laws in manufacturing IoT devices.

Where is the benefit of hi-jacking these devices in the first place? According to professional hacker Benjamin Särkkä there are different threat profiles for a politician or a top leader, when compared to a normal household (GoTech 2018a). This fact is also confirmed by author Järvinen when he was interviewed about the benefit of hacking smart home devices. He states that normal consumers are targeted only for the benefit of taking over the home computer and accessing its sensitive information. Spying a person’s computer is one objective for hackers. However, taking over a major company CEO’s, technical advisers, politicians or other significant individuals personal computers have larger pros than cons. They have enough network security for their computers at their workplace, but when they come home with their business laptops and connect them to the less protected home network, they become easy targets (GoTech 2018b).

Even if the computer is well protected, the IoT appliance connected to the same network usually are not. Hacking a home device just to cause damage to the household is highly unlikely. But there is still a possibility for it to happen, if these devices can be controlled remotely via network (GoTech 2018b). From potential financial information extracted from the victims’ network, hackers also benefit from the technological capacity of some IoT devices. Those devices that have enough performance can be utilized for mining cryptocurrency. These devices are used still for a financial gain but are used as a middleman to hide their crime.

As it was earlier stated, the responsibility is mostly in the hands of the consumer which is usually left alone to secure the smart IoT appliances from outside threats. It is also clear that consumers are not aware of these vulnerabilities and they trust in the manufacturers experience to make them safe, which is not guaranteed to begin with. Fortunately, there are cybersecurity companies that offer services to protect the home network without any additional stress. Consumer willing to invest to that kind of security unfortunately is not certain. Therefore, it is important to spread the word about the lack of security features which IoT appliances contain and inform consumers to take the security matter seriously.

2.2 Threats for companies

When it comes to companies, they are usually well protected from cyberattacks especially compared to typical home networks. Especially large companies have the finance and personnel to make their information security credible. However, there are real incidents involving smart IoT devices that exposed the companies' network to outside threats. One company was allegedly attacked due to coffee maker negligently connected to the same internal network as the company’s computers were using. Computers were used to control the factory’s production machines. Production in the factory was immediately forced into a halt. These computers were running an outdated XP operating system, which was not supported anymore (Bisson 2017).

Another case happened to a casino in North America. A fish tank was using a remotely controllable thermostat that had a vulnerability. Since the casinos network security was inadequate, hackers were able to exploit this weakness in the thermostat. The CEO of cybersecurity company Darktrace Nicole Eagan told in an interview that: “the hackers exploited a vulnerability in the thermostat to get a foothold in the network. Once there, they managed to access the high-roller database of gamblers and then pulled it back across the network, out the thermostat, and up to the cloud” (Wei 2018).

Those two cases are an example from a bad security design. Either it was unclear that these devices had outdated security settings, or the vulnerabilities were ignored due to lack of interest and neglect. This assumption is not farfetched, since company executives have little to none interest in their own network safety. At least according to the information security professionals surveyed by cybersecurity company RedSeal. Their survey reveals that “92% of all security teams had specific plans to protect and help their CEO from cyberattacks and data breaches. 54% of security personnel believe their CEO is ignoring these plans, potentially opening the door to cyberattacks” (Palmer 2019).

In addition, every tenth respondent stated that their own CEO had put the cybersecurity of their company at risk by making poor decisions or actions. 95% of the respondents are worried about IoT devices that are sold for consumers due to their bad cybersecurity and large portion of the respondents have no idea about the devices their CEO uses out of office. Some of the CEOs even have had no proper training in cybersecurity. According to the CTO of RedSeal Mike Lloyd, CEOs have wide range of accessibility inside a company. They have access to network resources and might think that same security rules concerning other workers do not apply to the highest place of the board. This is a huge risk for a company and people who want to take an advantage of the situation are free to blackmail, steal information or just conduct espionage on the company (Palmer 2019).

When it comes to household devices with IoT technology, it is safe to say that businesses are as much in danger as households. Businesses can be cyberattacked for various reasons and objectives in mind. That objective can be denial of service, disrupting system access and control, stealing or erasing data, damaging business equipment or breaching in to access private information. What is even worse that a security breach can cause financial loss, reputation might suffer, and identity of stakeholders could become compromised (Pal & Purushothaman 2017). If a company uses for example an internet-connected coffee maker or a vacuum cleaner, it needs to be protected as well as any normal computer. Otherwise, these IoT appliances or other devices utilizing sensors can be used as a gateway to access vital information.

2.3 Benefits of IoT for households

Since there are real vulnerabilities in IoT appliances that can cause serious damage to households and businesses, then why connect them to the network at all? There are in fact many benefits these IoT appliances can bring. The smart household technology starts to become worthy of the name when these devices are connected to the network and can be controlled with smart phones or with tablets. Therefore, being connected to the internet simply does not make them “smart enough”. It must be controlled remotely with something. Applications are specially designed to control and adjust settings of appliances remotely, which helps to command a vacuum cleaner to start cleaning the house before guests arrive, or ask a refrigerator to send a picture from the interior to see what groceries are needed for the guests (Gotech 2017a).

Having one IoT appliance in home environment does not significantly raise the efficiency in a household, but when there are large number of these devices inside one household, the benefits increase considerably (Gotech 2017b). The practicality of the home increases when the devices co-operate with each other making the house chores automated. Smart home devices can optimize houses energy consumption and increase financial benefit from it. This creates less carbon dioxide and is better for the environment (GoTech 2017c).

Especially IoT appliances improve the efficiency and quality of different activities that are carried out in households, such as cooking, cleaning and washing among other things. For example, according to the electronic device manufacturer Bosch, their coffee machine can be adjusted for personal needs. Using the Home Connect application it is easy to pre-order the

coffee to be ready at the exact time and different recipes can be found from within the application, so the coffee does not always taste the same. An oven can make perfect food when every dish has their own roasting program in the application (Bosch No date). Using the application ensures that the result of the consumers desired action will always be perfect and energy efficient.
Same type of manufacturers such as LG and Samsung offer similar solutions with their own products but add their own twists. LG offers portable LG Smart sensors that can be installed to non-smart appliances in order to make them operate as IoT devices. These sensors can measure temperature and humidity and send that information to the users SmartThinQ application where the user can apply adjustments (LG No date). Samsung on the other hand offers an option to control IoT devices via smart television in addition to their own application SmartThings. The application or the television can be used to control house devices such as lights or a washing machine without the need to get up from the sofa (Samsung No date).

These appliances can be controlled remotely but does that really give any significant improvement compared to not controllable ones? Is this hype about controlling remotely overrated and too enthusiastic? Leading researcher Timo Seppälä from the Research Institute of the Finnish Economy questions the benefits of smart home appliances. He states that there is no point controlling a coffee machine or a washing machine with a smartphone, if they need to be refilled manually. Some smart appliances might be useful in the future, but their long lifetime of usage slows their development (Leskinen 2019). There should be an actual advantage in controlling them remotely and not connecting them to the internet just for the fun of it.

2.4 Benefits of IoT for companies

Benefits that IoT can offer depends on the company itself. Since IoT does not apply only to household appliances and such, IoT does have benefits. As mentioned before, IoT sensors can be utilized to observe nearly everything that surrounds us. For example, manufacturing companies benefit from this technology greatly. IoT appliances might not give any prominent benefits for the manufacturing industry, but automated machines used in production surely will.

Quality control is one of those things that will improve from IoT. “It leads to higher customer satisfaction and reduced costs. Products are inspected to confirm that they have, for example, the appropriate color and that there are no defects. Using sensors to measure benchmarks that determine the performance and durability of the products is essential to avoid defects and ensure quality” (Workerbase 2019).

A property benefits from sensors that can monitor temperature inside the apartments and adjust it automatically to desired temperature. Carbon dioxide and moisture can also be monitored. In addition, the capacity of a warehouse can be monitored, access control can be surveilled, even tracking a parcels movement in real time is possible for a company to utilize (Digita promotional video 2016).

Some garbage disposal companies utilize sensors in trash bins for monitoring those which are full, and which are not. This allows the collector to empty only those trash bins that require it. It saves fuel costs and time, which every company needs. ABB utilizes IoT to change the performance settings of an industrial robot and control it remotely in the middle of its process. When it comes to benefits the possibilities are endless and only imagination is what restricts it. Sensors can be utilized to surveil all kinds of actions. “Any kind of machine, device, tool, property, vehicle or even a whole city are possible to be made smart utilizing sensors, communication, programs and analytics. Basically, it means that any kind of object can be transformed into a source of information, which offers completely new possibilities to bring value” (Ahvenlampi 2016). These are just few examples and there are many other ways to utilize sensors in business. When it comes to the value an IoT sensor can bring to a company, it definitely is worth of investing in, since it can bring a whole lot of value.

3 Research Methodology

For this thesis two interviews were conducted. One face to face interview was carried out at the workplace of the respondent and the other interview was carried out via e-mail. Questions were constructed case by case since the respondents area of expertise vary allegedly greatly from each other. For the respondents will they remain anonymous in this thesis and they are referred as company X and company Y.

Interview via email was surprisingly challenging and time consuming. Creating reasonable questions which are simultaneously related to the thesis subject took considerable amount of time. However, that was not the only problem. Finding and contacting the right professional was not efficient at all. The process of sending e-mails and receiving desired results required more patience than expected. Some potential respondents were interested at first about the subject but ended up being reluctant to answer after they saw the questions. Interview questions were therefore redesigned couple of times to get at least some research results. In the end results were received and they were enough.

It ended up being easier and more efficient to interview the desired person on the scene compared to an e-mail. People seem to check their e-mail in a variable fashion. In some situations, contacting via e-mail was carried out rather quickly, and the whole contacting process was pleasant. In some cases, however contacting took over one month, which was not ideal.

Many potential respondents were not willing to answer the interviews or were simply too busy to do so. It was surprisingly difficult to find a person willing to answer. Sometimes it was deeply unmotivating and the thesis came into a halt for a while. Fortunately, there was few respondents who agreed to take the interview.

Interview questions were constructed by taking into consideration the area of expertise of the respondents. The interview was performed in Finnish, since there was no guarantee of the language skills of the respondents. Also constructing the interview in Finnish language removed the risk of getting undesirable answers since sometimes somethings get lost in translation. Questions were open and gave a lot of room for the respondents to answer.

Interviews in general are defined as qualitative research methods. There are three types of interviews and they are structured, semi-structured and unstructured. They have different names among researchers and unstructured interview has the probably the broadest spectrum of names (Hirsjärvi et al 1997, 209). Unstructured interview is the same thing as open interview. “In-depth interviewing is a qualitative research technique that involves conducting intensive individual interviews with a small number of respondents to explore their perspectives on a particular idea, program, or situation” (Boyce & Neale 2006, 3).

In an open interview the interviewer tries to figure out the respondents’ thoughts, opinions, feelings and understanding whenever they appear along the conversation. Ordinarily an open interview takes a lot of time and it requires several tries. An open interview requires more skills than other interview methods (Hirsjärvi et al 1997, 209). Giving the option to the respondents to answer in their own words and language gave more comprehensive results for the interview, compared to a simple survey.

The big advantage of an interview compared to other research methods is that it can be adjusted when the situation requires it and it helps with agreeing with the respondent. It is possible to adjust the order of the interview subjects and there are more options to analyze the answers than for example with post questionnaires. Many matters that are assumed to be upsides of an interview include problems as well. Creating an interview requires thorough planning and preparing to the role of an interviewer, which takes time. Interview also might include many false sources, which are caused by the interviewer as well as by the respondent and the interview situation. The respondent might experience the interview as threatening or scary in many ways (Hirsjärvi et al 1997, 205, 206).

However, there are more weaknesses for an open interview. They “are usually the least reliable from research viewpoint, because no questions are prepared prior to the interview and data collection is conducted in an informal manner. Unstructured interviews can be associated with a high level of bias and comparison of answers given by different respondents tends to be difficult due to the differences in formulation of questions" (Research Methodology No date).

Reliability of the interview might be weakened by the fact that it is a habit for people to give socially acceptable answers. The respondent may give information about specific subjects even when the interviewer does not ask for it. The respondent for example wants to appear as a proper citizen, as a knowledgeable and cultural person, morally as well as socially obedient person. Instead of these next features that are often kept silent: illness, deficiency, criminality, acting against norms or financial situation (Foddy 1995, 118).

Gathered data can be analyzed in many ways, but they can be categorized roughly in two ways. To explaining approach and to understanding approach. In explaining approach, statistics analyzing and drawing conclusions are used. In understanding approach, a qualitative analysis and drawing conclusions are used. In qualitative research analyzing especially is considered difficult. There are a lot of choices and there are no restrictions. The most ordinary qualitative analysis methods are thematic analysis, typification, content breakdown, discourse analysis, conversation and interaction analysis (Hirsjärvi et al 1997, 224).

Thematic analysis is used in this thesis as an analyzing method. “Thematic analysis aims to identify the essential topics or themes forming the data” (Jyväskylän Yliopisto 2010). Using this method to compare interviewees answers to each other’s and to already existing sources. Information about IoT, which has been gathered earlier is compared to the results given by the respondents, in order to detect recurring themes and vice versa. Inductive reasoning as analyzing method is additionally used in this thesis. Since only two interviews were conducted and the questions were constructed directly to them, thematic analysis would not be enough.

In inductive reasoning it all starts with “specific observations and measures” which help to find “patterns and regularities”. These findings are then used to develop “general conclusions or theories” (Trochim 2006). Analyzing the collected data using these two methods in order to identify reoccurring topics concerning IoT turned out to be the right choice. They are more productive analyzing methods for this thesis compared to other methods, since lot of different sources were used. Interview questions were first and foremost designed to reveal the respondents’ preparedness to the spreading technology of IoT and how they are planning to adapt with it, or have they already done so.

4 Results of company X

Results from the interview of company X´s respondent gave a perspective from a retailer's point of view. They work with consumers of IoT home appliances every single day and they are experts of understanding the situation from a customer's perspective. This interview was held on the premises of the retailer. The aim of interviewing a retailer was to find out the consumers interests and criteria when buying an IoT home appliances. And are they interested about the safety of the product or are they interested about other aspects? In addition, it was important to find out if retailers are helping consumers to secure their appliances.

From a retailer's point of view the amount of smart home devices has increased in every device category. According to the respondent for company X the amount of smart televisions is over 90 percent, which means that almost every television in the market has the capability to connect to the internet. 50 percent of small devices such as sound systems and speakers have these capabilities. Smart household appliances are still in the minority, but their amount is slowly increasing.

Since it has been stated that consumers are not adequately protecting their network devices it was important to question the service procedures company X offers for their consumers. It is clear, that retailers are in a key position to influence the customers attitude against home network security. Company X is aware of this and it is a common practice to train their employees to instruct their customers to protect their home devices properly. Even the manufacturers of smart home appliances arrange training sessions for retailers about the features and other aspects of the devices. This develops and enhances the customer service greatly when employees are up to date.

It also common for the employees to offer security products such as security routers and ask consumers about their antivirus programs, if they have one or if it is up to date. Their goal is to emphasize that everything must be frequently updated in order to maintain their home network security credibility. If the customer states that everything is in order, then security subjects are not discussed any further. Main goal is to maintain a professional service experience for the customer and not force anyone to buy any certain products. Company X´s respondent claimed that the price of the network security products could be the reason for many unprotected devices, and it is not simply worth it to invest in security. They do not see the benefits they would get from investing in additional security, and they have a fear that they would pay for nothing.

According to Company X´s respondent the customer is often unaware about the state of their network security and do not know the proper procedures to protect them. Some customers are aware but are not interested to invest into their home network security. Main criteria for customers while buying a new product usually is the including features and what the device is capable of. For example, in a television the quality of the picture or how user friendly it is, are the most important features the customers look for. Some customers can be interested about the safety features but in some cases new technological features are intriguing, hence customers want to get their hands on those devices.

Company X´s respondent agrees that it would bring more value to the service, if there would be a small instruction brochure given with a smart home device. In the brochure there would be simple step by step guide on how to increase the safety of a home network. Although some manufacturers offer some instructions within their device’s manuals, there would be no harm for such brochure, which would increase knowledge about the importance of network safety.

The benefit which comes with the smart home devices in company X´s opinion is huge. The devices can be optimized according to the need of the consumer. According to the company X´s respondent for example a washing machine can be controlled with a cell phone and command it to perform a program for a certain fabric material for a perfect result. Oven can be commanded to use a cooking program crafted for a certain meat in order to make the end result always perfect. In addition, they consume less energy and water which saves money.

Approximately in 10 years company X´s respondent evaluates that in most of sold home devices will have internet features implemented, since they aspire to enhance everyday life. There is little to none risks when using these home devices, if the security aspect is thoroughly taken care of. And if the security side is inadequate, then it is always an option not to connect them to the network. These IoT home devices are safe to use, if they are used correctly. When done so the benefits of using them indeed exceed the risks.

4.1 Results of company Y

Company Y’s respondent interview was conducted via e-mail. Since the respondent is working in IoT business, the questions were constructed that aspect in mind. However, there were some similar questions that were asked in the interview of the company X’s respondent. Aim of the IoT professional’s interview was to find out benefits and risks of IoT for a company, and how profitable IoT technology is for a company. In addition, the professional’s personal opinions about IoT appliances and their effects on households was asked. Even though the respondent does not directly work with household appliance IoT, the respondent’s experience and expertise about IoT is comprehensive.

According to the Company Y’s respondent businesses benefit from their IoT technology couple of ways. Their long-range wireless area network technology allows businesses to gather information with sensors from infrastructure, properties and devices nimbly, but most importantly cost-effectively utilizing long lasting batteries. Both businesses and households benefit from this technology, since it enhances the installation progress of a device and it saves money. There are always risks for new technology solutions, but using right methods in the right way, these risks can be controlled according to the respondent.

For example, the company Y's IoT technology uses its own network to transfer data between the devices. Their IoT systems are totally separated from the internet and do not use the normal internet protocol to transfer data, which means that the risks are relatively small. They are also separated from internal networks of businesses, so if that internal network is compromised, it does not have an impact on the IoT network. The IoT network therefore cannot be attacked straight through them. When the company Y's respondent was asked about the responsibility of the network's safety, the respondent replied that the responsibility is always on the service provider. However, the user of the service is also responsible on using the product correctly and not to neglect the intentional use. Cyber security aspect must always be up to date on both parties in order to minimize the risks.

When the respondent was asked about the future of the IoT technology, there was no doubt that it will become more common in households and businesses. They become part of used devices and some benefits on different devices are more noticeable than on others. IoT solutions bring new possibilities, since it can increase the performance of a company or it can redefine the way a business operates. That way a company can gain an advantage on others, but it is not a guarantee that every existing company would benefit from it or need it at all.

When it comes to households, IoT solutions bring new yet easier and cost-effective appliances to facilitate everyday life. From security aspect all normal appliances used in household and business environment are tentatively safe when installed, if the technology is confidently reliable. Investing in a cheap IoT device increases the risks excessively because their level of security cannot be verified. Basically, if the knowledge how to use IoT is safely is ensured, there should not be any serious consequences.

4.2 Summary of the results

Comparing the respondents results a few certain opinions came up in both cases. Both respondents claimed that the appliances, which utilize IoT are broadly safe to use. They also agreed that households and companies mostly benefit from IoT and the related risks are not too severe, if the user knows how to properly secure them. Energy efficiency, time saving, and convenience were the occurring themes in both interviews. Which is a sign from that they know enough about IoT. They were certain about the benefits of IoT appliances, but they were not worried about the cybersecurity aspect, even though smart appliances are generally inadequate in this regard.

They both seem to trust IoT devices even though many IT professionals are concerned about it. Partially it is understandable because manufacturers have improved the network safety of IoT devices, well at least when it comes to the biggest manufacturers. Retailers might be more positive about IoT since they must know the basics of network security in order to provide better customer service. However, being too positive towards IoT is not advised. Devices might have vulnerabilities due to bad encryption or coding, which means that no matter how secure the network is, the device itself is not.

The positivity of IoT professional towards this technology is probably due to their own IoT service which utilizes a separated network. When their sensors are using another network to transfer data instead of the internet, the risks are drastically lower. That is why the installation of the sensors must be precise, since a single mistake might endanger the network. This requires complete isolation from company networks and from the internet. However, the professional was exceptionally positive that IoT device is safe, if the technology is ensured as safe when installing it. The retailer was also positive that some IoT devices from China for example possibly have notably inferior security features than their European counterparts.

Despite being too optimistic they are not wrong about the inadequate knowledge base of people when it comes to cybersecurity. Cases when people have been cyberattacked has been a result of ignorance about network security. Some of these cases could have been prevented if the owners were more aware about the risks. Information about the importance of cybersecurity should be transmitted more frequently and make a basic network security a mandatory requirement in every household and in every company. Spreading the word in a way that it influences and effects in the mind of an individual is a difficult challenge. News about threats of IoT simply will not make people to invest network security.

5 Conclusion

First, when it comes to IoT technology it is constantly spreading and connecting with everything. Hospitals, companies, properties, cars and appliances among many others are being affected by this. Clearly IoT improves especially communications between parties, by utilizing sensors that give information in real time and do it automatically. These sensors can be programmed to observe temperature, surroundings, consumption or even fullness of a trash can, just to name a few. Business expenses decrease while efficiency of work increases.

Basically, the possibilities are endless since sensors can be used to measure anything. It is also a useful feature that this type of technology can be automated. They could learn and detect certain patterns rather soon. For example, a normal morning routine becomes a lot faster when all appliances communicate with each other. Alarm clock wakes up the person and communicates with a coffee maker and command it to start brewing while television goes on and informs the person about morning news. They simply have the capability to make everyday life partially automated and more timesaving.

There are many benefits IoT brings for private companies and public sector but what about appliances? To be fair actual appliances are still a minority compared to other devices that utilize IoT technology. For example, sensors that measure temperature or energy consumption have been used a long time now. Then again it is difficult to draw the line between what is a smart appliance and what is not. Generally, in media a normal toaster for example that has internet connection is listed as an IoT device, despite the lack of sensors. In general, it might be confusing that IoT appliances are referred as smart appliances because IoT means that there are sensors implemented in the appliance additionally to the internet connection. Still it is not wrong to call an IoT appliance as smart, since despite that they differ technically from normal smart appliances, they are still smart, but in a way just a little smarter. However, the definition of IoT is not clear either, because there are many different explanations for it. It seems like people do not completely understand what really makes a device as an IoT device. The term IoT itself is very confusing when smart appliances mean basically the same thing for most people.

Appliances benefit from IoT as much as any other devices. They can exchange information with the owner via smart phone about their tasks and status. For example, a refrigerator informs that a product inside the fridge is about to expire and recommends buying a new one or an oven can be commanded to prepare a meal according to a recipe found from a cooking website. Again, there is a lot of room to develop appliances that make living more effortless. IoT appliances alone are an effective addition for their owners but they really start to shine when the number of these appliances increase in a household. When they can communicate with each other the benefits only increase.

Threats of IoT technology has been an occurring subject in media in this decade. Especially for consumers the poor security has brought many issues. Although the security aspects of these appliances have been improved in last few years, there still are problems that occur to this day. First problem is related to user behavior. When a consumer decides to buy a smart appliance the usual questions that matter for them are how user friendly it is, what is the price and how useful it is. The safety of the product is not the main concern among consumers despite the constant news about threats of IoT. At home they plug it in and start to use it, sometimes even ignoring available software updates. There are also other problems with user behavior. Using the factory password for Wi-Fi router and not changing it at any point, re-using same passwords in too many places and having outdated programs on computer and appliances, which then give an opportunity for criminals to breach into the home network.

Second problem is the appliances themselves. Especially cheap ones and products bought from China or other places outside Europe Union have worse security features which cause threats for home network security. Even some appliances cannot be updated after they are bought. This is due to lack of legislation concerning smart appliances. Manufacturers are making these devices without any restrictions and consumers are in principle left alone to secure their devices. Only recently EU has recently woken up to consider some legislation concerning IoT appliances to ensure standard security features to every manufactured appliance.

The General Data Protection Regulation or GDPR determines what personal information a company can collect, handle or retain from a person (Euroopan Unioni 2019). This regulation ensures that companies inside and outside EU respect the privacy of a citizen of EU and it demands companies to make their IoT devices and services safer to use. Unfortunately, this regulation is associated only with the countries inside EU and not others.

When it comes to businesses, threats are the same as they are for households. However, businesses tend to have proper cybersecurity. Appliances used in businesses are not such a big of a threat, but accidents do happen. Sloppy installation of an appliance to the business network or poorly secured appliance still can cause issues for a company. Businesses must be vigilant of a product they are planning to purchase and ensure that the device is safe to use. In addition, CEO’s and other key officials of a company are a risk for their own companies outside of the office.

People tend to work remotely sometimes and connect their work laptop into a home Wi-Fi. These Wi-Fi connections are vulnerable or at least not as secure as in companies. It is often forgotten that having reliable cybersecurity does not just apply in workplaces, but it must be as active at home too. These CEO’s and other key personnel endanger their companies unintentionally and are a serious threat. Negligence and ignorance cause security threats for companies and individuals alike. Human error gives the opportunity for these kinds of attacks to happen. It is therefore important to keep up with the development of IoT in order to secure it.

What then can be done in order to use IoT appliances more safely? First, avoiding any cheap IoT appliances on the market. If the company which manufactured the appliance is small or unpopular it is plausible that it has poor security or no security at all. The home router password should be changed from the factory password and additionally using different passwords on every website. One effective way to increase home network security is to create a separate network for smart appliances, so that computer stays in its own. In case an appliance is compromised the computer stays safe where the valuable information is stored.

This protects identity and other credential information, but it does not stop criminals using an appliance for a DDOS attacks or for mining cryptocurrency. Fortunately, there are some cyber security companies that offer services for protecting all devices connected to the same network. Security routers and artificial intelligence is used to detect malicious behavior if someone is without permission trying to access these devices. These cybersecurity programs additionally keep smart devices and the computer up to date, so that the consumer has less things to worry about. If all these facts are noticed and network security is taken seriously in a household, it is very difficult for anyone to gain access to the IoT appliances.

Do benefits exceed the risks then? IoT appliances are very handy and efficient, and the risks become a minor nuisance when security is taken seriously in a household. Is there a need for these kinds of appliances? Not everyone will need that kind of technology in their home. Even if the technology is very convenient to use and it improves living standards. Some appliances are unlikely to ever benefit from being smart. Especially those appliances that you need to manually refill like washing machine or a dish washer, there is no proper benefit of it being smart. Then again if a person just wants to control everything with a smart phone, no one is there to stop it. Only if there will be no more ordinary appliances for sale, then it will become a necessity in every household.

To capsulize the current situation of IoT appliance security, it is not on a satisfying level. Even though the International Electrotechnical Commission has published international IoT standards, laws concerning manufacturing of IoT appliances are still very inadequate, so it is not certain what kind of security an appliance has. Since standards are guidelines and not compulsory to follow, many manufacturers are not interested to use them. It is in the consumers responsibility to ensure that the appliance is safe to use and usually people do not do that. People’s knowledge about home network security should be somehow increased. It is not a simple task, but people are beginning to understand its importance. When do people start to take it seriously? To end it in quoting the words of F-Secure’s director of research Mikko Hyppönen, “When people in the 90’s realized that malicious software spread, it became normal that these kinds of attacks occur everywhere. It required continuous attacks against computers until people started to protect their devices. This might require a similar global phenomenon towards IoT appliances in order to people start protecting their appliances” (MTV Uutiset 2018).

References

Printed Sources

Foddy, W. 1995. Constructing questions for interviews and questionnaires. Theory and practice in social research. 3rd edition. Cambridge: Cambridge University Press.

Hirsjärvi, S. Remes, P. Sajavaara, P. 1997. Tutki ja kirjoita. Helsinki. Kustannusosakeyhtiö Tammi.

Pal, A. Purushothaman, B. 2017. IoT: Technical challenges and solutions. Boston. Artech House.

Smith, S. 2017. The internet of risky tings: Trusting the devices that surround us. Sebastopol. O'Reilly Media Inc.

Electronic Sources

Ahvenlampi, K. 2016. Miten Internet of Things muuttaa yritysten liiketoimintaa?. Digitalist, 25 February. Accessed 12 April 2019. https://digitalist.global/talks/miten-internet-of-things-muuttaa-yritysten-liiketoimintaa/

Avast. 2018. Avast 2019: Extends Artificial Intelligence Technology to Block Advanced Phishing Attacks for Enhanced Consumer Security. 10 October. Accessed 24 April 2019. https://press.avast.com/avast-2019-extends-artificial-intelligence-technology-to-block-advanced-phishing-attacks-for-enhanced-consumer-security

Banks, T. 2018. IoT Security – Should consumers bear any responsibility?. Timothy M Banks IT and Data Governance. 11 September. Accessed 24 August 2019. https://timothybanks.com/2018/09/11/iot-security-should-consumers-bear-any-responsibility/'

Bisson, D. 2017. How a Smart Coffee Machine Infected a PLC Monitoring System with Ransomware. Tripwire. Accessed 19 January 2019. https://www.tripwire.com/state-of-security/ics-security/how-a-smart-coffee-machine-infected-a-plc-monitoring-system-with-ransomware/

Bosch. No date. Stories: Bake #LikeABosch. Accessed 12 February 2019. https://www.bosch.com/stories/bake-like-a-bosch/

Bosch. No date. Stories: Wake up #LikeABosch. Accessed 12 February 2019. https://www.bosch.com/stories/wake-up-like-a-bosch/

Boyce, C. & Neale, P. 2006. Conducting in-depth Interviews: A Guide for Designing and Conducting In-Depth Interview. Pathfinder International Tool Series. Accessed 25 June 2019. http://www2.pathfinder.org/site/DocServer/m_e_tool_series_indepth_interviews.pdf

Check Point software technologies ltd. 2017. HomeHack: How Hackers Could Have Taken Control of LG's IoT Home Appliances. 26 October. Accessed 19 January 2019. https://blog.checkpoint.com/2017/10/26/homehack-how-hackers-could-have-taken-control-of-lgs-iot-home-appliances/

Euroopani Unioni: Sinun Eurooppasi. 2019. Yleinen tietosuoja-asetus. 14 October. Accessed 8 November 2019. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm

Fruhlinger, J. 2018. The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet. CSO, 9 March. Accessed 20 May 2019. https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

F-Secure. No date. IoT Connected Life. Accessed 21 January 2019. https://www.f-secure.com/en/web/home_global/connected-life

Gilchrist, A. 2017. IoT Security Issues. Boston. Walter de Gruyter. Book from ebook central. Accessed 14 February 2019. https://ebookcentral.proquest.com/lib/laurea/reader.action?docID=4810138

Gotech: Kaikki Kodintekniikasta. 2017a. Älykäs kodintekniikka avuksesi: miksi kodinkoneita kannattaa ohjata älypuhelimella. 5 November. Accessed 12 January 2019. http://gotech.fi/2017/11/05/kodinkoneiden-alypuhelinohjaukseen/

Gotech: Kaikki Kodintekniikasta. 2017b. Älykäs kodintekniikka avuksesi: älykodista on paljon hyötyä asukkaille. 30 November. Accessed 12 January 2019. http://gotech.fi/2017/11/30/alykoti-kuluttaja/

Gotech: Kaikki Kodintekniikasta. 2017c. Älykäs kodintekniikka avuksesi: kodinkoneiden paikka on internetissä. 29 November. Accessed 14 January 2019. http://gotech.fi/2017/11/29/alykas-kodintekniikka-internetissa/

Gotech: Kaikki Kodintekniikasta. 2018a. Älykäs kodintekniikka avuksesi: esineiden internet hakkerin silmin. 30 April. Accessed 12 January 2019. http://gotech.fi/2018/04/30/alykas-kodintekniikka-iot-tietoturva/

Gotech: Kaikki Kodintekniikasta. 2018b. Älykäs kodintekniikka avuksesi: tietokirjailija Petteri Järvinen arvioi älylaitteiden tietoturvaa. 16 March. Accessed 14 January 2019. http://gotech.fi/2018/03/16/alykas-kodintekniikka-avuksesi-petteri-jarvinen/

International Electrotechnical Commission. No Date. International Standards (IS). Accessed 8 November 2019. https://www.iec.ch/standardsdev/publications/is.htm

IoT:lla tasaista asumismukavuutta VVO-konsernin kohteissa Espoossa. 2016. [video]. Digita. Accessed 14 June 2019. https://www.youtube.com/watch?v=ipgSPQWywso

Jyväskylän Yliopisto. 2010. Thematic Analysis. 8 March. Accessed 5 June 2019. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/en/methodmap/data-analysis/thematic-analysis

Kerrigan, S. 2018. The History Behind the 15 Kitchen Appliances That Changed The Way We Live. Interesting Engineering, 13 April. Accessed 8 April 2019. https://interestingengineering.com/the-history-behind-the-15-kitchen-appliances-that-changed-the-way-we-live

Leskinen,M. 2019. Mitä tapahtui esineiden internetille, josta piti tulla seuraava iso mullistus? Kehitys vei eri suuntaan ja eri nopeudella kuin ennustettiin. Yle Uutiset, 26 September. Accessed 30 September 2019. https://yle.fi/uutiset/3-10985702

MTV Uutiset. 2018. Puutteellinen tietoturva voi mahdollistaa käyttäjien vakoilun tai autovarkaudet – tämän takia kukaan ei puutu IoT-laiteiden riskeihin. 15 May. Accessed 20 May 2019. https://www.mtvuutiset.fi/artikkeli/puutteellinen-tietoturva-voi-mahdollistaa-kayttajien-vakoilun-tai-autovarkaudet-taman-takia-kukaan-ei-puutu-iot-laiteiden-riskeihin/6907902#gs.82acw6

Niiler, E. 2019. How the Second Industrial Revolution Changed Americans' Lives. History, 25 January. Accessed 18 February 2019. https://www.history.com/news/second-industrial-revolution-advances

Palmer, D. 2019. Cybersecurity: Is your boss leaving your organisation vulnerable to hackers?. ZD Net, 15 July. Accessed 26 July 2019. https://www.zdnet.com/article/cybersecurity-is-your-boss-leaving-your-organisation-vulnerable-to-hackers/

Research Methodology. No date. Interviews. Accessed 25 June 2019. https://research-methodology.net/research-methods/qualitative-research/interviews/#_ftn1

Samsung. No date. Smart Home: Älykäs koti ja esineiden internet. Accessed 16 February 2019. https://www.samsung.com/fi/smart-tv/smart-home-with-iot-devices/

SmartThinQ Developer. No date. LG SmartThinQ. Accessed 16 February 2019. http://thinq.developer.lge.com/en/discover/lg-smartthinq/

Tompkins, B. 2018. How Smart Appliances Can Unlock Their IoT Potential. IoT for all, 11 September. Accessed 25 May 2019. https://www.iotforall.com/unlock-smart-appliances-iot-potential/

Trochim, W. 2006. Deduction & Induction. Web Center For Social Research Methods, 20 October. Accessed 6 June 2019. https://www.socialresearchmethods.net/kb/dedind.php

Uusitalo, K. 2019. Leivänpaahtimet osallistuvat kyberhyökkäyksiin Suomessakin – Mitä kuluttajan pitää tietää älylaitteensa tietoturvasta?. Yle Uutiset, 16 July. Accessed 24 August 2019. https://yle.fi/uutiset/3-10880289?fbclid=IwAR3OKefNVFchUYrJDB7xksPdSUYc80dnhLXC4ZslxYPQZhU1imMQ4wYFRv0

Wei, W. 2018. Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer. The Hacker News, 16 April. Accessed 12 March 2019. https://thehackernews.com/2018/04/iot-hacking-thermometer.html

Workerbase. No date. 5 Benefits of IoT in Manufacturing. Accessed 8 May 2019. http://www2.pathfinder.org/site/DocServer/m_e_tool_series_indepth_interviews.pdf

Appendices

Appendix 1: Interview questions for company X

1. Do you have more smart household devices on sale compared to the ordinary ones? Have the number of smart devices increased?

2. IoT appliances sold to households are according to many professionals dangerous to consumers, since their network security is nonexistent or very weak. Are the employees instructed about the safe usage of IoT appliances and do they inform customers about the importance of securing them with proper actions or does the responsibility lie with the consumer?

3. Are the employees trained about the network security threats of smart appliances, so that they are aware and know how to protect them?

4. Do you see it necessary to educate your employees to understand the importance of having a reliable network security in a household and maintaining it?

5. When a customer comes to buy a smart appliance, what are his/her usual requirements while choosing it? Is he/her interested about the safety features or about something else? For example, about the price?

6. Do you see smart appliances as a better choice for consumers compared to a ordinary one? Why?

7. Do you sell or recommend buying an antivirus program or for example a security router with a smart appliance? If you don’t, would it be viable?

8. Could it be reasonable to give a free small manual with a smart appliance, where proper security guidance would be instructed to the customer? It would give step by step instructions clearly on how to build a believable network security for a home.

9. Is it possible that you would exclusively sell IoT appliances for customers? Or do appliances that cannot be connected to the internet always have a demand?

10. In your own opinion, are there some certain appliances, which should not be connected to a network in home environment? Appliances like a washing machine or door locks?

Appendix 2: Interview questions for company Y

1. In what way do companies benefit from your IoT technology services?

2. Does using your IoT technology have any risks for companies?

3. Could the IoT technology you are providing benefit ordinary households? Would ordinary homes benefit as much as companies do?

4. Appliances that are connected to a network like vacuum cleaners and thermostats have been abused to access consumers or business information. Could someone utilize your IoT technology to access business networks and that way to sensitive information?

5. Does a company using your IoT technology have the responsibility to protect it or is the responsibility on the service provider?

6. What is your vision concerning the future of IoT technology? Will it become necessary for companies and homes to utilize, or will some of them manage without it?

7. Could IoT technology completely replace all sorts of appliances used in home and business environment? Could it be possible that every device would work via network at a workplace or at home in the future?

8. In your own opinion, are there some certain appliances, which should not be connected to a network in home or business environment? Appliances like a washing machine or door locks?