Cybersecurity and the Internet of Things

IDSI31421: Applied Cybersecurity Strategy for Managers

Trimester 3 – July 1, 2016

Submitted by

BAKER Sarah B00682183

FRISON-ROCHE Grégoire B00470386

KUNCIKOVA Barbora B00689703

Introduction/Abstract

The Internet of Things (IoT) is a topic that gets a lot of attention and has become somewhat of buzzword in business and technology today. In many ways, this hype and excitement is not misplaced, as IoT has fascinating implications and opportunities for both consumers and businesses. However, the cybersecurity threats that this explosive growth represents are sometimes overlooked or not clearly understood. This paper will introduce the concept of IoT, including the definition, trends and applications. The next section will discuss the potential cybersecurity risks for IoT, for both industries and consumers. Finally, the last section will discuss recommended preventative measures and defense mechanisms available, while considering the fast changing nature of IoT technology.

What is the Internet of Things?

The past decades have seen huge advances in electronic communications, from the rise of the Internet to the ubiquity of mobile devices. However, this communication is now shifting from devices that simply connect users to the Internet, to communication linking the physical world to the cyber world (Borgia 2014). Generally speaking, this notion is called Cyber-Physical Systems (CPS) and includes technologies such as (i) automation of knowledge work, (ii) Internet of Things, (iii) advanced robotics, and (iv) autonomous/ near-autonomous vehicles (Borgia 2014). However, IoT is considered to be the CPS technology with the largest expected economic impact (McKinsey Global Institute 2013).

Given IoT is one of the most talked about trends in IT, there are as many definitions of the phenomena as there are angles to study. The origins of the concept IoT can be traced back to a group at MIT, who defined it as "an intelligent infrastructure linking objects, information and people through the computer networks, and where the RFID technology found the basis for its realization'' (Brock 2001). Today, IoT extends far beyond RFID technology. A more recent definition describes IoT as "a highly interconnected network of heterogeneous entities such as tags, sensors, embedded devices, hand-held devices and back-end servers" (Malina et al. 2016). The International Telecommunication Union (ITU) describes IoT as "anytime, any place connectivity for anyone... connectivity for anything. Connections will multiply and create an entirely new dynamic network of networks – an Internet of Things'' (ITU 2005).

Therefore, the defining attribute of IoT is that it involves *things*, moving beyond networked computers, tablets or smartphones to include just about any physical object that can be connected and communicate (Barajas, 2014). The value offered by IoT comes from the fact that these objects- which are not machines, and do not function like machines- are able to gather and communicate data, which means information can be translated into action at astounding rates (Burras, 2014). The concept behind IoT was aptly captured back in 1999:

> "If we had computers that knew everything there was to know about things — using data they gathered without any help from us — we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things

> needed replacing, repairing or recalling, and whether they were fresh or past their best. The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so" (Ashton, 1999).

The reason IoT is now growing so rapidly is that technology has evolved enough to be able to support the connectivity required for IoT to really take off. For example, cloud computing enables the transmission of data from sensors to applications which can analyze it in real-time, providing the real value behind IoT (Burras, 2014). Other enabling technologies include the introduction of IPv6 (allowing billions of communication addresses), ubiquity of wireless chips in a range of devices, improved mobile data coverage and superior battery technology (EY, 2015).

Given this enabling technology, IoT is poised to be a powerful disruptor. McKinsey has identified IoT as one of the top twelve most economically disruptive technologies, noting that there has been a 300% increase in connected machine to machine devices in just five years (from 2008 to 2013) (McKinsey Global Institute 2013). They estimate the potential economic impact of IoT to be between 2.7 to 6.2 trillion by 2025 (McKinsey Global Institute 2013) and see implications as wide-ranging as increased quality of life for individuals, creation of new products and services for businesses and bolstered economic growth and productivity for governments and economies (McKinsey Global Institute 2013).

Applications of the Internet of Things

IoT Applications can be broadly split into industrial and consumer use. Despite the fact that consumer IoT tends gain the most attention, industrial IoT is actually more advanced than consumer IoT. As one CSO pointed out "The Internet of Things is not new. For the past 25 years — ever since the development of microprocessors and network-based instruments — companies in the process industries such as oil and gas, chemicals, refining, pharmaceuticals, manufacturing and mining have been avidly exploring how to use sensors to make their processes more reliable, efficient and safe" (Zornio, 2015). The concept of IoT has therefore been in use in commercial spaces for a long time but the sophistication of these networks are increasing drastically, and with it, comes better information for decision making.

For example, Virgin Atlantic is now using highly connected planes, where "literally every piece of [the] plane has an internet connection, from the engines, to the flaps, to the landing gear. If there is a problem with one of the engines we will know before it lands to make sure that we have the parts there…each different part of the plane is telling us what it is doing as the flight is going on" (Finnegan, 2013). This represents a massive amount of data which can be analyzed to schedule proactively identify potential issues, plan maintenance, and identify operational efficiencies. However, it also represents a vulnerability for hackers to exploit. If every piece of the plane has an internet connection, there are thousands of opportunities to gain access to the plane's systems.

While better information for decision making is a big advantage, the true value of IoT comes from its potential to disrupt established industries, creating new services and new products.

Consider the rise of Zipcar and other car sharing companies – by utilizing sensors and network connections in cars, they are able to rent cars for short time spans to registered members, eliminating the need for a staffed rental office and gaining the ability to optimize each car's use for higher revenues (Chui, Löffler & Roberts, 2010). However, having access to this volume of sensitive customer data (matching location with customer profiles for example) represents large privacy obligations on behalf of the company.

From a consumer perspective, the general categories for IoT include wearables, smart metering, automotive, home automation and medical devices (Greverie, Buvat, Nambiar, Appell & Bisht, 2014.) Wearable tech is probably the best known example of IoT, with many people choosing to track their activity levels, heart rates, sleeping patterns and other personal data via Fitbits, Apple Watch or any of the other myriad of devices available. However, many consumers are unaware that their (extremely) personal data may be synced or stored unencrypted (Drolet, 2016). Home automation can offer many convenient benefits, including automating lights, controlling HVAC systems or securing door locks. It can also offer peace of mind to new parents, who can use IoT baby monitors to view a live-stream of their babies on their smart phone. However, most parents aren't aware that they might be exposing their homes to cybercriminals, as demonstrated by a recent case of hackers gaining access to a baby monitor and using it to scope out the house and plan a burglary (EY, 2015). This last example shows the possible intersection between cybercrime and traditional crime.

These are only a few of the many examples of IoT applications for businesses and consumers. Experts acknowledge that the potential for IoT is huge. "We're only really scratching the surface of what IoT can become. There are massive benefits for businesses and society at large" (Qualtrough, 2014). All these possibilities and applications of IoT make it a fascinating field to study, however, as IoT grows, so do the cybersecurity risks of having a massive network that will be interwoven into our personal, private and government activities. The following section will outline the cybersecurity threats, followed by a presentation of defense mechanisms and solutions.

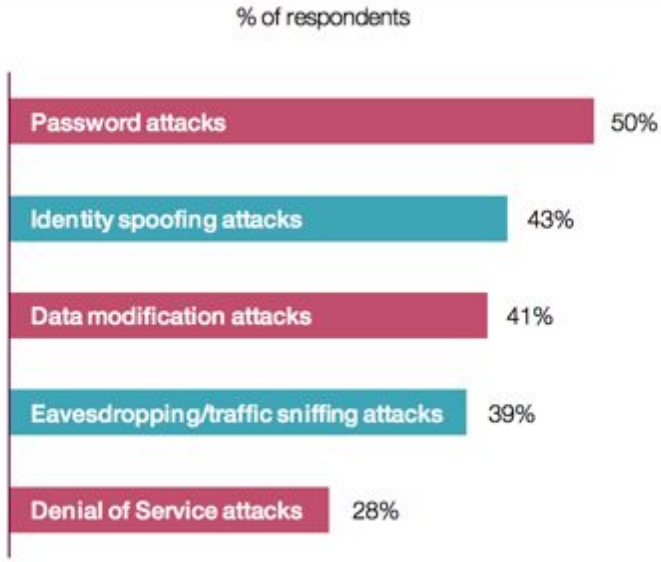
Cybersecurity Threats

As the examples above demonstrate, the potential cybersecurity threats of IoT are growing at the same fast pace of the IoT industry as a whole. Researchers estimate that by 2020, there will be over 50 to 60 billion active wireless connected devices all over the world (Reger, 2014). These connected devices represent an incredible amount of data which can be easily misused if not protected well. Additionally, the increase in connected devices results in more possible attack vectors and so naturally, IoT devices become an increasingly attractive target for cybercriminals. It is important to consider the security issues of IoT now, before security issues become an obstacle.

As previously mentioned, the two major markets for IoT are consumer and enterprises. The forecast for 2018 says that 70% of the installed IoT base will focus on the demands of enterprises and will account for 90% of IoT spending (Press, 2015). What is interesting is that

both consumer and industrial users face the same threats, but with different impacts. For example, companies generally gather a larger volume of sensitive data than consumers would at an individual level. Therefore, when a security breach occurs or information (such as company know-how or customer data) is compromised, it has a greater impact on industry, competition, customers and many others. That is one of the reasons why industrial IoT users need to be concerned not only about the IoT they employ in their manufacturing or other operational processes, but also IoT products designed for the consumer market. Capgemini has identified the top security threats to IoT product as password attacks, identify spoofing attacks, data modification attacks, eavesdropping/traffic sniffing attacks and denial of service (DOS) attacks (Greverie, Buvat, Nambiar, Appell & Bisht, 2014).

Figure 1: Top Security Threats to IoT Products



Source: Capgemini Consulting and Sogeti High Tech, "Security in the Internet of Things Survey", November 2014

N=109

While there is wide variation in the types and uses of IoT devices, there are some common threads to the cybersecurity threats posed. These common threads are described in the next sections.

24/7 ON - Constant connection, actualization of security system

Unlike personal computers or smartphones which can be easily turned off, connected devices are often on 24 hours a day and 7 days a week. The constant connection offers an opportunity for attackers to gain access to homes, offices, labs or factories for a long period of time. Once devices are connected into the network, they are using the exact same protection throughout these long-running sessions. This demonstrates the need for more efficient protection. Existing security is insufficient or ill-suited to address the risks inherent with the ubiquitous deployment of IoT devices. McKinsey estimates that the cost of ineffective cybersecurity will reach $3 trillion by 2020 (Gault, 2016).

Recent examples of hackers remotely controlling the Jeep Cherokee car (Greenburg, 2015) or medical devices are only the tip of the iceberg. However, the positive side effect of these security breaches is that people are becoming more aware of privacy and security issues, which naturally follows great inventions. So far, it is still at the beginning of epoch of IoT, which means that the opportunities are evolving and the possible threats are being discovered. For that reason, things cannot be rushed.

Limited operational system to carry anti-malware

There is a considerable percentage of IoT devices which are not capable of running anti-malware software due to the insufficient operating system or the missing infrastructure needed to support such applications. Fighting an advanced cyber attacks would have been absolutely impossible. They are missing the processing power and space to store databases of malware definitions. That might be a hint for developers of IoT security to look for different solutions, such as securing of IoT ecosystems, platforms, whole networks, which can provide the background for users to control and protect their connected devices against malware.

Large platforms and huge repositories of stored IoT data

Because of the incapability of many devices to carry anti-malware software, there is a question how to secure other parts of the IoT system. Many companies like Microsoft, IBM and Cisco have developed large platforms for this purpose. But the more data they gather, the more attractive it appears to cybercriminals. Creating a detailed profile about any individuals in the world can have very serious consequences such as leading to spying, robberies, industry espionage, political discrediting and many others. Cloud services with vast databases of personal information gathered for a long period of time and from many connected devices represents a source of income for cybercriminals. If a data leak occurs from one device, the impact may be minimal, or barely harmful. What creates the biggest danger is the combination of many data in wrong hands, who can build a very exact profile. This creates circumstances which infringe tremendously on privacy if hackers are able to follow the data trail. One study found that organizations typically provide information on the types of data collected, and how data is shared with third parties, but it is much more rare for organizations to provide information on the degree of user control (ability to opt-in or out of data collection and sharing) or information on how data is managed after a service is terminated (Greverie, Buvat, Nambiar, Appell & Bisht, 2014).

Low awareness about potential risks between consumers

Even though security and privacy issues are vastly spreading among consumers, there is very little attention paid to these issues. Once in a while, there is a report of a customer data leak of some company. These stories tend to create a buzz for a while but in the long run, the level of awareness and caution of consumers remains quite low. It is human nature to avoid proactively planning for these kinds of abstract risks, and individuals tend not to worry about these risks until it becomes a problem for them, at which point they have already been the victim of cybercrime.

Providing a basic education about security of IoT and the Internet in general would be an ideal way to increase the awareness of cybersecurity risks. By starting this education with school-age children, who will spend their entire life connected by IoT devices, the next generations would be equipped with knowledge about possible threats and securing their privacy. One VPN provider has already responded to this need by creating an "I Spy" book for children, which focuses on educating primary age U.K. school kids about the darker side of IoT (Lomas, 2016).

Insufficient legal background for processing data from IoT

Even though IoT has been here for several years, many countries have no laws which would include IoT devices. In that case, general privacy laws come into account (which were frequently created long before anyone had ever heard of IoT). These laws vary from country to country. The European Commission passed the General Data Protection Regulation to standardize data privacy laws across the whole of Europe, but the laws will not take effect until 2017 (Talbott, 2016). In general, there are great differences in privacy laws across the world and some kind of standardization should be taken into account.

Another question includes the readiness of the public Internet, which is considered to be a global networking medium for IoT solutions. At this time, it provides a little in a sense of service-level agreement (SLA) and quality of service (QoS) guarantees (latency, reliability, security, availability) (Sherman, 2016).

Leaving backdoors for "good people" leaves backdoors for "bad" ones as well

This issue became a hot topic in the US recently due to the proceedings between the FBI and Apple with regard to gaining access to the phone of a suspected terrorist (Benner & Lichtblau, 2016). So far, cases have mostly revolved around governments seeking data from PCs and smartphones, but with the continued growth and expansion of IoT, it is only a question of time before data from connected devices becomes the subject of a government inquiry as well. Devices as Microsoft Kinect or Amazon's Echo are "listening" and "watching" all the time, so they collect a tremendous amount of data that could potentially be of interest. One point of view suggests that collecting this data is acceptable, if it helps catch some "bad people". But in the same time, it raises the question of civil liberties and the right to privacy. Additionally, the issue of *Quis custodiet ipsos custodes,* or who will guard the guards themselves? Leaving the door open leads to many potential opportunities for misuse, even if the original intention is benign. Therefore, the security of private data should be a top priority and the focus should be on the best possible way how to reach that.

Giving devices so much access to private information gives a certain level of discomfort to many. However, the value of many IoT devices comes from their ability to collect and make sense of data, so without opting to share information, there are very few benefits available to users. Adoption of IoT to day-to-day life is very delicate and heavily depends on trust in device makers, network and platform providers, government. Hence, if devices don't meet consumer expectations for privacy, they will fail because customers will choose not to use them. Security breaches will gravitate towards the weakest link in the chain. However, even when vulnerabilities are discovered, the low cost of the devices may disincentivize producers

from issuing security patches. Therefore, there is a need to look for balance in ensuring sufficient protection of data within the producers' and providers' capabilities.

IoT user protection

Privacy issues

One of the most regularly quoted fears about IoT is privacy concerns (Capgemini, 2005; CREDOC, 2007) and worries of an abusive and massive use of personal data by societies, organizations or governments without a clear knowledge of what is used, by who and in what purpose. Privacy concerns cover a range of issues such as a prohibited or unauthorized use of personal data available (bank cards, mobile phones, loyalty cards, access cards, health cards, video surveillance, etc.), the ability to track individuals (GPS system, access cards...) and their actions, as well as data gathering and processing for police surveillance or marketing profiling.

Some technical solutions have emerged to respond to the need for protection of privacy. One of the most common and simplistic but effective solution is an "opt-in" which consists of explicitly asking the authorization of the user before sending an e-mail, a SMS or gathering information about the user (coming and moving in a website, type of purchases, profile, method of payment for example). This also includes the compulsory or optional deactivation of a specific function such as geolocalization.

More innovative solutions have been developed along these lines but are not in widespread use yet (Benghozi, 2009). For instance, in the US there is a passport "cage de Faraday" innovation which prevents anyone from reading the microchip unless the passport is open. The CASPIAN association (Consumer Against Supermarket Privacy Invasion) advocates for the neutralization of tags outside the store. Following this, RSA security has developed a blocker tag in 2003 which prevents the unauthorized reading of a microchip. Open Business Innovation has created a private mode to allow the user to control his microchip and the information available. In the same vein, the Distributed Systems research group from the Swiss Federal Institute of Technology in Zurich has developed a watchdog tag which allows user-controlled identity management by providing the chip reader, its localization etc. on a screen or a mobile phone. This allows the user to control his partial identities depending on the situation (facing a physician, a friend...) thanks to a specific code for each partial identity, for instance with different usernames and passwords. But this solution is relatively difficult to use because it requires a great deal of memorization. A more flexible initiative was created at the University of Berne with the concept of virtual person which works with a virtual mask to protecting user identities. One mask covers several people and each person can use several different masks, configured to handle in their name. RFID Guardian has launched a firewall project which aims to blur the RFID wave thanks to a small battery integrated into mobile phones or laptops.

Encryption is also a powerful tool for privacy, and has gained interest recently due to the fact that it may protect users against massive surveillance from governments. Encrypted data are

coded with the help of an algorithm and become illegible to unauthorized personnel. The only individuals who can decipher and read these data are the ones who possess a specific decryption key. The encryption solution is already available on computer, laptops, tablet and Smartphone. It is a very reliable technology: with a software like PGP, if the encryption key uses 1024 ou 2048 bits, it is virtually impossible for an external person to read the message. This is because it would require dozens and dozens of powerful computer during several years to find the key (Les Echos, 2016). With the application Telegram, the conversation is encrypted and automatically destroyed at the end, which means you need the key to decode the conversation necessary in real time.

With the extent of connected devices, data collected on individuals are growing. Some countries have established a right to be forgotten (2009 in France, 2014 in the EU) to allow the erasure of personal content from the internet. The advent of the IoT is a real challenge from a legal perspective to maintain and even amplify these rights. This raises questions on the legal status of personal data, the exercise of consent, functional deactivation, etc. The right has to evolve to better embrace the specificities of IoT and correctly respond to the new issues it raises.

Securing IoT

Aside from the privacy of information shared or collected via IoT devices, the security of IoT is pressing issue. Documentation about the potential risks of IoT is plentiful but frequently ignored or underestimated by both consumers and business. Sensitization about this theme is a crucial point to upgrade IoT security. Too many companies are not aware of the dangers they are exposed to. Securing the IoT chain aims to fight against malware, bugs, hacking, and industrial spying, amongst others.

Reducing the exposure of connected devices to attacks is a complex task. It requires an architectural knowledge of the value chain that links things to the cloud. It must consider devices themselves, their sensors and processors, local and remote networks, protocols and servers at any level, their software and data processing operations that are carried out there. From a consumer perspective, the French telecom giant Orange provides some tips for securing IoT (Orange website, 2016).

- Ensure devices are updated with the latest version of software and that passwords have been changed
- Ensure Wi-Fi routers are secure with regards to their names, passwords, and required updates
- Complete an inventory of all connected devices and their localization to identify any suspicious activities
- Replace obsolete devices as needed (when manufacturers stop providing patches for software, etc. (Kaspersky Lab, 2015))
- Know what information is collected by each connected device in under to understand how information is managed, protected and used
- Stay vigilant 24/7: firewalls and anti malware do not offer total protection

From a managerial perspective, the Open Web Application Security Project (OWASP) has published sixteen principles of IoT security (Miessler & Smith, 2016). OWASP is a not-for-profit charitable organization that functions as an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. Their key principles of IoT security include ideas such as the importance of testing for scale (as security measures that protect an ecosystem may create a self denial of service at a IoT scale), verifying data to prevent autonomous misinformation from corrupting a system, using autonomous system's tolerance for monotonous, and tedious operations as a security advantage, carefully considering the full data lifecycle in order to encrypt data uniformly, planning for the worst by building capabilities to respond to adverse events before they occur, and recognizing the need for IoT ecosystems to address evolving security concerns over the extended lifespan of the device (Miessler & Smith, 2016).

Enterprises at the cutting edge of technology have understood the threats of IoT and already taken action to protect sensitive data. However securing IoT represents a huge investment in time and money, and only these firms can support such developments. The best way to ensure IoT security is to revamp the product development process to address security issues from the very beginning (Greverie, Buvat, Nambiar, Appell & Bisht, 2014). For some companies without technical expertise, a packaged solution could be the answer waiting for the upgrading of their own system by designed solutions. However, standardization may lead to a new risk: everyone capable of breaking one system can have access to a large set of systems. Obviously this would have different consequences for devices which contain sensitive or potentially dangerous information (for instance, car networks), versus IoT objects like connected toothbrushes or coffee makers (which do not hold sensitive data but are still at risk of a bug or serving as an entry point to more sophisticated devices on the same network).

Conclusion

Securing IoT will be an ongoing process which requires a lot of time, as new issues will become apparent as new technology is introduced, and as users gain familiarity with issues. Looking back on historical innovations, each new technological wave brings new vulnerabilities. For example, It took decades to secure rail, air and motor transport. The seat belt, invented in the late 19th century, only became compulsory in France in 1973. Today's vehicles carry standard safety features that were cutting edge innovations ten years ago. In the digital field, these innovation-securing cycles have accelerated and will continue to grow.

However, users ultimately need to be aware of the privacy and security risks associated with IoT and manage their usage accordingly. IoT devices offer incredible benefits and opportunities for both individuals and enterprises but these advantages must be balanced with appropriate risk management steps to fully capture the value offered by IoT.

References

Benghozi, P.J., Bureau, S., Massit-Folléa, F. (2009). The Internet of Things. Paris: Éditions de la Maison des sciences de l'homme.

Benner, K., & Lichtblau, E. (2016). U.S. Says It Has Unlocked iPhone Without Apple. *New York Times*. Retrieved from http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0

Borgia, E, (2014). The internet of things vision: Key features, applications and open issues. *Computer Communications*, 54, pp.1–31. Available at: http://dx.doi.org/10.1016/j.comcom.2014.09.008.

Brock, D.L. (2001). The Electronic Product Code (EPC) – A Naming Scheme for Physical Objects, White Paper, Retrieved from http://cocoa.ethz.ch/downloads/2014/06/None_MIT-AUTOID-WH-004.pdf

Caron, X., Bosua, R., Maynard, S.B., Ahmad, A. (2016). The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective, 15. Retrieved from http://www.sciencedirect.com/science/article/pii/S0267364915001661

Evans, J. (2016) "6 conseils pour sécuriser l'Internet des objets" *Orange Business Services*. Retrieved from http://www.orange-business.com/fr/blogs/securite/bonnes-pratiques/6-conseils-pour-securiser-l-internet-des-objets

Finnegan, M. (2013). "Boeing 787s to create half a terabyte of data per flight, says Virgin Atlantic" *Computer World UK*. Retrieved from http://www.computerworlduk.com/news/data/boeing-787s-create-half-terabyte-of-data-per-flight-says-virgin-atlantic-3433595/

Gault, M. (2016). Rethinking security for the Internet of Things. *TechCrunch*. Retrieved from https://techcrunch.com/2016/05/06/rethinking-security-for-the-internet-of-things/

Greenburg, A. (2015). Hackers Remotely Kill a Jeep on the Highway—With Me in It. *Wired*. Retrieved from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Greverie,F., Buvat, J., Nambiar, R., Appell, D., & Bisht, A. (2014). Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT. *Capgemini Consulting.* Retrieved from https://www.capgemini-consulting.com/resource-file-access/resource/pdf/securing_the_internet_of_things.pdf

Grondin,A. (2016) "Le chiffrement des données, comment ça marche?" *Les Echos*. Retrieved from

http://www.lesechos.fr/18/02/2016/lesechos.fr/021707218117_le-chiffrement-des-donnees--comment-ca-marche--.htm

International Telecommunication Union. (2005). ITU Internet Report 2005: The Internet of Things, International Telecommunication Union. Retrieved from https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf

L. Atzori, A. Iera, G. Morabito. (2010). The internet of things: a survey, Comp. Netw.: Int. J. Comp. Telecommun. Network. 54 (15) 2787–2805.

Lomas, N. (2016) "IoT Security Turned Into an "I Spy" Educational Book for Kids" *TechCrunch*. Retrieved from https://techcrunch.com/2016/01/27/iot-security-turned-into-an-i-spy-educational-book-for-kids/

Malina, L. et al. (2016). On perspective of security and privacy-preserving solutions in the internet of things. *Computer Networks*, 102, pp.83–95.

McKinsey Global Institute. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy*, Retrieved from http://www.mckinsey.com/~/media/McKinsey/Business Functions/Business Technology/Our Insights/Disruptive technologies/MGI_Disruptive_technologies_Executive_summary_May2013.ashx.

Miessler, D. & Smith, C. (2016). Principles of IoT Security. Open Web Application Security Project. Retrieved from https://www.owasp.org/index.php/Principles_of_IoT_Security

Newman, R. et al. (2016). Web 2.0—The past and the future. *International Journal of Information Management*, 36(4), pp.591–598. Retrieved from http://www.sciencedirect.com/science/article/pii/S0268401216301712.

Press G. (2015). "9 new prediction and markets assessments for Internet of Things" *Forbes Tech*. Retrieved from http://www.forbes.com/sites/gilpress/2015/07/30/9-new-predictions-and-market-assessments-for-the-internet-of-things-iot/#610ccd827203

Qualtrough, E. (2014). "Internet of Things needs government push, says BT CIO" *CIO UK.* Retrieved from http://www.cio.co.uk/it-networking/internet-of-things-needs-government-push-says-bt-cio-3572796/

Reger J. (2014). "The threat and opportunity of Internet of things*" Global Intelligence for the CIO*. Retrieved from http://www.i-cio.com/big-thinkers/dr-joseph-reger/item/the-threat-and-opportunity-of-the-internet-of-things

Sherman, D. (2016). "How ready is the Internet for IoT" *TechCrunch*. Retrieved from https://techcrunch.com/2016/05/26/how-ready-is-the-internet-for-iot/

Talbott, A. (2016). "Privacy Laws: How the US, EU and others protect IoT data (or don't)" *ZDNet*. Retrieved from http://www.zdnet.com/article/privacy-laws-how-the-us-eu-and-others-protect-iot-data-or-dont/