ASSESSING THE THREATS AND OPPORTUNITIES OF THE EMERGING INTERNET OF THINGS MARKET

UFCFE6-15-3 LESSON 2

ALEXANDER LORD

10 DEC 2018

Table of Contents

INTRODUCTION

The Internet of Things refers to "*objects with computing devices in them that are able to connect to each other and exchange data using the internet*" (Cambridge University Press, 2008). For example, the Internet of Things might involve a refrigerator ordering new groceries when its inventory is low.

Arm, the company I am working for during my placement, is one of the leading contributors to the currently emerging Internet of Things market. Arm's primary business model involves designing chips for small embedded devices (like mobile phones and Internet of Things devices). They then sell these designs to other companies and earn royalties off the devices sold. Arm consider themselves to be at the heart of the market – providing chips, operating systems and development tools to companies designing Internet of Things devices. They boast "*an ecosystem of more than 1000 partners, with more than 125 billion Arm-based chips shipped to date*" (Arm Holdings, 2018).

One of the biggest opportunities of the Internet of Things is revenue generation. "*The Internet of Things will help to improve business efficiency*" (Atlantic BT, 2018), as well as open brand-new markets. The largest (and most obvious) threat of the Internet of Things is security and privacy. As more devices become connected to the internet and to each other, more security gaps appear.

I will use various pieces of literature, internet sources and personal, to identify the most prominent threats and opportunities of Internet of Things. From here on, I will refer to the Internet of Things as "IoT".

METHODOLOGY

I started my research by going onto the UWE library website to look for books on the Internet of Things. Although the library has several books on it, they were all very similar. There was very little variation in what the books were talking about in relation to IoT. I read parts of one book by (Buyya, 2016) and moved onto internet sources.

I went to look for professional journals online. I found it surprisingly hard to find any, and when I did, they were either confusing to access, or restricted. I stopped looking for journals and moved onto standard internet sources.

I found the bulk of my material from Google searches. A lot of large, reputable websites have articles discussing IoT, and its threats and opportunities. These articles presented findings from either their own research, or from studies that they had read. This helped me to find more sources of information.

I also conducted a SWOT analysis to provide a clear outline of the strengths and weaknesses of IoT. This can be found in the "Findings" section, under "SWOT Analysis".

LITERATURE REVIEW

Opportunities

The biggest attraction of IoT is the rapidly expanding market. As IoT is a relatively young market, there are still a lot of money-making opportunities for companies. According to market research,

"the IoT and M2M market will be worth approximately $498.92 billion by 2019. The value of the IoT market is expected to hit $1423.09 billion by 2020." (RnRMarketResearch, 2014). (Buyya, 2016) stated that "*The increase of investment in IoT by developed and developing countries hints at the gradual change in strategy of governments by recognizing IoT's impacts and trying to keep themselves updated as IoT gains momentum*". The fact that governments are using their own money to research and fund IoT, would suggest that it has a serious potential for growth, offering lots of opportunities in a multitude of spaces. Singapore has announced its intention to be the first smart nation by investing in smart transport systems (Yu, 2014).

IoT offers instant access to data and information that was either previously inaccessible or very hard to access, especially to the average person. Wearables are a very popular example. In fact, (Lasse Lueth, 2015), the founder and CEO of IoT Analytics, conducted research into the applications of IoT. They found that wearables were the second most popular application, behind smart homes. Wearables are used generally to transmit medical data to a doctor or to a user's mobile device. The most common examples are FitBit and Apple Watches. These can track, record and transmit data such as heart rate, steps and sleep pattern.

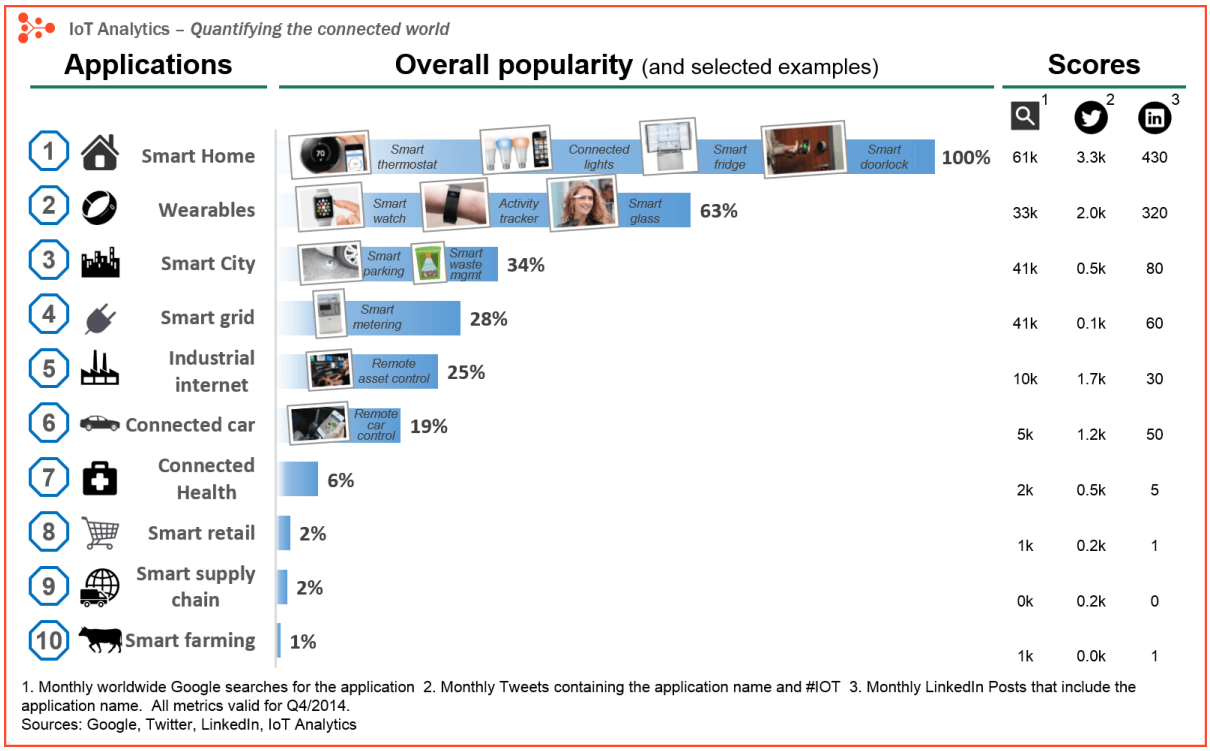

Figure 1 - https://iot-analytics.com/wp/wp-content/uploads/2015/03/IoT-application-ranking-v3-min.png

I also read an article posted on Forbes that discussed the opportunities of IoT. (Saran, 2018) stated that "*IoT is transforming the health industry.*" He provided two examples of how IoT is being used for remote health monitoring; such as the Hexoskin biometric shirt and the Jawbone UP3 fitness tracker. He argued that "*Patients also benefit from the technology as it provides an effective and economical substitute for on-site clinical nursing.*" He even went as far as to predict that "*by 2020, the worldwide smart health care industry will grow to almost $170 billion."* This shows that the emergence of IoT won't be restricted to technology markets but will also be useful to other industries. Saran summed it up simply - "*IoT is blurring industry borders.*"

Threats

One threat or issue related to IoT is the amount of data and the complexity of dealing with it. IoT devices and sensors can produce extortionate amounts of data very regularly. Companies need to be able to not only deal with this data, but also be able to utilize it for the benefit of their business. IoT devices produce 5 quintillion bytes of data produced *every day* (that's 2.5 followed by 18 zeros) (Stack, 2018).

The largest threat of IoT is security and privacy. Security is one of the most discussed topics in technology. Personal or confidential data can be leaked if organizations do not have good enough security. A big example is the hacking of Home Depot in 2014. Credit card data was stolen for more than 50 million customers and cost the company $179 million in settlements (Roberts, 2017). This wasn't an issue directly with an IoT device but shows that many organizations don't have strong security protocols in place for their software and hardware systems. "This is the IoT equivalent of having a username/password combo of "admin" and "password" (Atlantic BT, 2018). Atlantic went on to suggest that these security concerns often make it difficult to persuade stakeholders to buy into the IoT. The costs and risks often out-weigh potential for success.

FINDINGS

Statistics

The IoT market has provided excellent opportunities for Arm, who design microprocessors. In fact, most smaller devices (like mobile phones), tend to run on an Arm-based processor. This made IoT devices the perfect opportunity for Arm's low-powered chips. Arm recently acquired Treasure Data, in a move towards creating end-to-end IoT services. Arm is "*no longer scoring the IoT opportunity in mere billions of devices (as before) but is now predicting a world of a trillion connected devices by 2035*" (Scales, 2018).

NewGenApps collected a cohort of statistics regarding the future business potential of IoT. "*A whopping $19 trillion is anticipated as cost-savings and profits from this investment.*" Although this seems like a massive number, "*Only 0.06% of all devices that could potentially leverage IoT are actually doing so. This makes the remaining 99.94% available for optimization*." This further shows the true potential expansion that the IoT market has. (NewGenApps, 2018)

Intel, one of the leaders in the market, expect that "*by 2025 the global worth of IoT tech is projected at $6.2 trillion"* (Intel, 2018). NewGenApps also discussed specific markets that use IoT, stating that *"the maximum value from healthcare ($2.5 trillion) and manufacturing ($2.3 trillion).*" They continued with, "*the market for smart cars and connected cars is also a huge market. The percent of internet connected cars is expected to rise from 10% in 2012 to a whopping 90% by 2020*" (NewGenApps, 2018). These three markets can be seen in figure 1 on the previous page.

Barcelona is the perfect example of how advantageous smart cities can be. Following the 2008 recession, Barcelona harnessed technological solutions to save the city money, whilst also creating jobs and opportunities. In 2015, the Barcelona City Council sponsored 12 smart city programs that created or maintained 1,870 jobs. The projects delivered €43 million worth of benefits between 2011 – 2014, with an expectation to grow to €832 million by 2025. Besides creating jobs and saving money, they also save 9,700 tons of CO2e and 600,000 liters of water each year (Lopez, 2014). Maybe every city should take a leaf out of Barcelona's book.

SWOT Analysis

STRENGTHS	WEAKNESSES
Innovation Simplify Tasks More Access to Data & Information Reduce Costs	Security Challenges of Managing Big Data Large Investment Risks
OPPORTUNITIES	**THREATS**
Healthcare Benefits Opportunity for Large Investment Return Big Data can provide Valuable Insights Smart Cities can Save Money	Vulnerable to hackers / attacks Hesitation due to Privacy Concerns Government Regulations / Legal Concerns

DISCUSSION

The study conducted by RnRMarketResearch in 2014 estimated that the market value of IoT would be "*$498.92 billion by 2019."* This research is quite outdated, especially considering how much the market has grown in the past 5 years. A much more recent prediction argues that the market could reach "*$745 Billion in 2019, surpassing the $1 trillion mark in 2020 and reaching $1.1 trillion in 2021"* (IDC, 2019). This shows an even larger scale of growth than was predicted 5 years ago.

IoT is expected to do wonderful things for the healthcare industry and has already provided incredible new insights into how doctors can obtain and monitor medical data from patients. However, it could be argued that the financial benefits are more relevant to the United States of America (USA). As the majority of healthcare in the USA is private, the healthcare sector will see more of a direct profit compared to locations like the UK, where healthcare is free. Although IoT can help the NHS save money, the profits will be lower than that of the USA. It may also be worth noting that the healthcare related financial estimations used in this report thus far, are in US dollars ($).

Despite the current security risks, Forbes expects the security of IoT devices to increase in 2019. IoT devices are vulnerable to hackers and security threats. Forbes states that "hardware manufacturers like Cisco, HPE, Dell and more are building specific infrastructure for the edge deigned to be more physically rugged and secure" (Newman, 2018). It could also be argued that as more devices become connected to the Internet of Things, the larger the security risk will be. The apparent lack in security for IoT devices could also be a massive opportunity for business. The obvious lack in security has opened a market that needs to be filled. I imagine companies would pay top dollar for reliable end-to-end solutions.

As Arm is at the center of the industry's largest IoT ecosystem, they have invested a lot of time and effort into making IoT devices more secure. The aim is to ensure that security is not an option and that devices in every sector are acceptable secure (Arm Holdings, 2018). Being at the center of this ecosystem gives Arm the best advantage to the IoT security market.

For example, Arm's mbed IoT device platform is often used for development on IoT devices. This comes bundled with uVisor, which works by shielding critical peripherals from the outside (Arm

Holdings, 2018). Arm's TrustZone technology provides security for CPU's. This is often used for device authentication (Arm Holdings, 2018). Device authentication is a major security issue with IoT devices. Devices often connect or communicate with each other without much, if any, authentication. This would provide a pretty open network for hackers. Arm's Platform Security Architecture (PSA) provides a common framework for companies to use when developing devices. This makes security even easier to implement and leaves little room for excuses (Arm Holdings, 2018).

CONCLUSION & RECOMMENDATIONS

Generally, the predictions show that the IoT market still has exponential growth to come and there is no expectation for the market to plateau or degrade. Specific sectors, such as healthcare, manufacturing, wearables and smart cities are expected to be among the most profitable from IoT.

Whilst doing my research, I noticed that the financial predictions for the IoT market can vary quite drastically between different pieces of research. Although the specific number changes, I think the most important point to takeaway here is that the market is growing. There is no doubt about it.

Although the market leaders are the typical big technology companies (Arm, Intel, IBM, etc.), companies of any size, in any sector, will be able to use IoT devices for any reason. Increasing profits, reducing outgoings, and generating big data are among three of the most beneficial advantages of IoT. Security, however, is by far the largest risk for IoT devices, for any company. Although security is being improved, the risk is constantly growing, and this should be at the forefront of any company's decision to use IoT.

Newcomers to IoT should consider the hardware devices, the software platforms and the companies that they use and buy from. Different companies offer differing services and varying advantages. Utilizing the full support of the industries experts will be crucial in making IoT work for any business. Diving head-first into an IoT project, without proper guidance on security and usage, could lead to profit loss and a bad reputation.

The key themes and takeaways of this report have been; to demonstrate the business opportunities that IoT can provide; but possibly more importantly – the security risk that comes with these investments. Poorly secured devices could lead to a massive investment loss.

Bibliography

Arm Holdings, 2018. *Arm.com.* [Online]
Available at: https://www.arm.com/company
[Accessed 6 January 2019].
Arm Holdings, 2018. *Mbed OS.* [Online]
Available at: https://www.mbed.com/en/platform/mbed-os/
[Accessed 21 January 2019].
Arm Holdings, 2018. *TrustZone.* [Online]
Available at: https://developer.arm.com/technologies/trustzone
[Accessed 21 January 2019].
Arm Holdings, 2018. *Why Arm Security Architecture.* [Online]
Available at: https://www.arm.com/why-arm/architecture/platform-security-architecture
[Accessed 21 January 2019].
Atlantic BT, 2018. *ATLANTIC BT.* [Online]
Available at: https://www.atlanticbt.com/insights/3-threats-and-3-benefits-of-the-internet-of-things/
[Accessed 7 1 2019].
Buyya, R., 2016. Internet of Things: Principles and Paradigms. In: R. Buyya & A. Vahid Dastje, eds. *Internet of Things: Principles and Paradigms.* Melbourne: Morgan Kaufmann, p. 341.
Cambridge University Press, 2008. *Cambridge Dictionary.* [Online]
Available at: https://dictionary.cambridge.org/dictionary/english/internet-of-things?q=Internet+of+Things
[Accessed 5 January 2019].
IDC, 2019. *IDC Forecasts Worldwide Spending on the Internet of Things to Reach $745 Billion in 2019, Led by the Manufacturing, Consumer, Transportation, and Utilities Sectors.* [Online]
Available at: https://www.idc.com/getdoc.jsp?containerId=prUS44596319
[Accessed 19 January 2019].
Intel, 2018. *A Guide to the Internet of Things.* [Online]
Available at: https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html
[Accessed 19 January 2019].
Lasse Lueth, K., 2015. *IoT Analytics.* [Online]
Available at: https://iot-analytics.com/10-internet-of-things-applications/
[Accessed 8 January 2019].
Lopez, J., 2014. *Barcelona 5.0,* Barcelona: s.n.
NewGenApps, 2018. *13 IoT Statistics Defining the Future of Internet of Things.* [Online]
Available at: https://www.newgenapps.com/blog/iot-statistics-internet-of-things-future-research-data
[Accessed 18 January 2019].
Newman, D., 2018. *Five IoT Predictions For 2019.* [Online]
Available at: https://www.forbes.com/sites/danielnewman/2018/07/31/five-iot-predictions-for-2019/#77e27fc06edd
[Accessed 19 January 2019].
RnRMarketResearch, 2014. *Markets and Markets.* [Online]
Available at: https://www.marketsandmarkets.com/Market-Reports/iot-application-technology-market-258239167.html
[Accessed 7 January 2019].
Roberts, J. J., 2017. *Fortune - Here Are 10 of the Biggest Corporate Hacks in History.* [Online]
Available at: http://fortune.com/2017/06/22/cybersecurity-hacks-history/
[Accessed 9 January 2019].

Saran, J., 2018. *Forbes - Where IoT Applications Are Creating Investment Opportunities For Entrepreneurs.* [Online]
Available at: https://www.forbes.com/sites/theyec/2018/08/24/where-iot-applications-are-creating-investment-opportunities-for-entrepreneurs/#5277d4da2a77
[Accessed 8 January 2019].
Scales, I., 2018. *ITUNews.* [Online]
Available at: https://news.itu.int/arm-pelion-iot-end-to-end-platform/
[Accessed 17 January 2019].
Stack, T., 2018. *Internet of Things (IoT) Data Continues to Explode Exponentially. Who Is Using That Data and How?.* [Online]
Available at: https://blogs.cisco.com/datacenter/internet-of-things-iot-data-continues-to-explode-exponentially-who-is-using-that-data-and-how
[Accessed 22 January 2019].
Yu, E., 2014. *Singapore unveils plan in push to become smart nation.* [Online]
Available at: https://www.zdnet.com/article/singapore-unveils-plan-in-push-to-become-smart-nation/
[Accessed 7 January 2019].