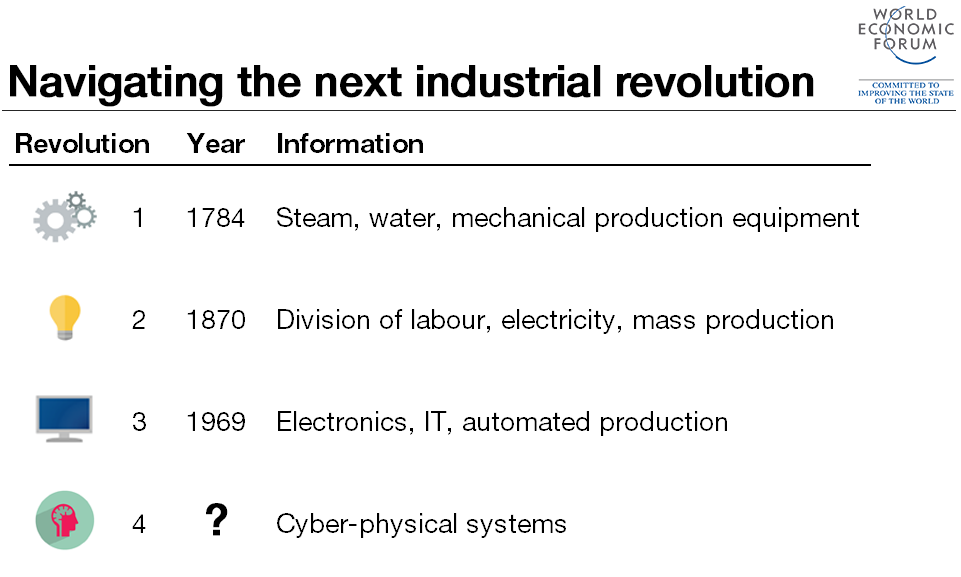
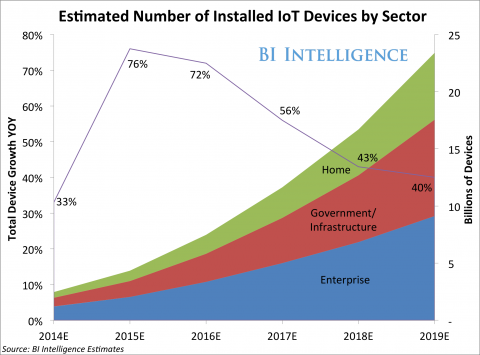
Dissertation Intro

The internet as we know it has undergone many transformations since its invention in the late1960s as a part of the third industrial revolution to the creation of the world wide web by Tim Berners-Lee in 1990, to the present day, where the current development of the Internet of Things represents the newest development of the internet and is being considered by many as the possible fourth industrial revolution alongside artificial intelligence.



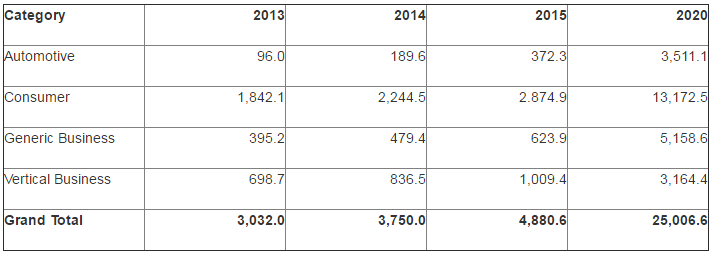
**Figure 1 – Fourth Industrial Revolution - World Economic forum**

Although the expansion of IoT has been well documented, many mainstream media outlets fail to inform the general population on what IoT actually is. As simply defined in the oxford dictionary the Internet of things is; “The interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data” (Reference). These interconnected everyday objects or “smart devices” which form the building blocks of IoT can come in any shape or form and can benefit domestic, enterprise and even governmental/infrastructure markets.



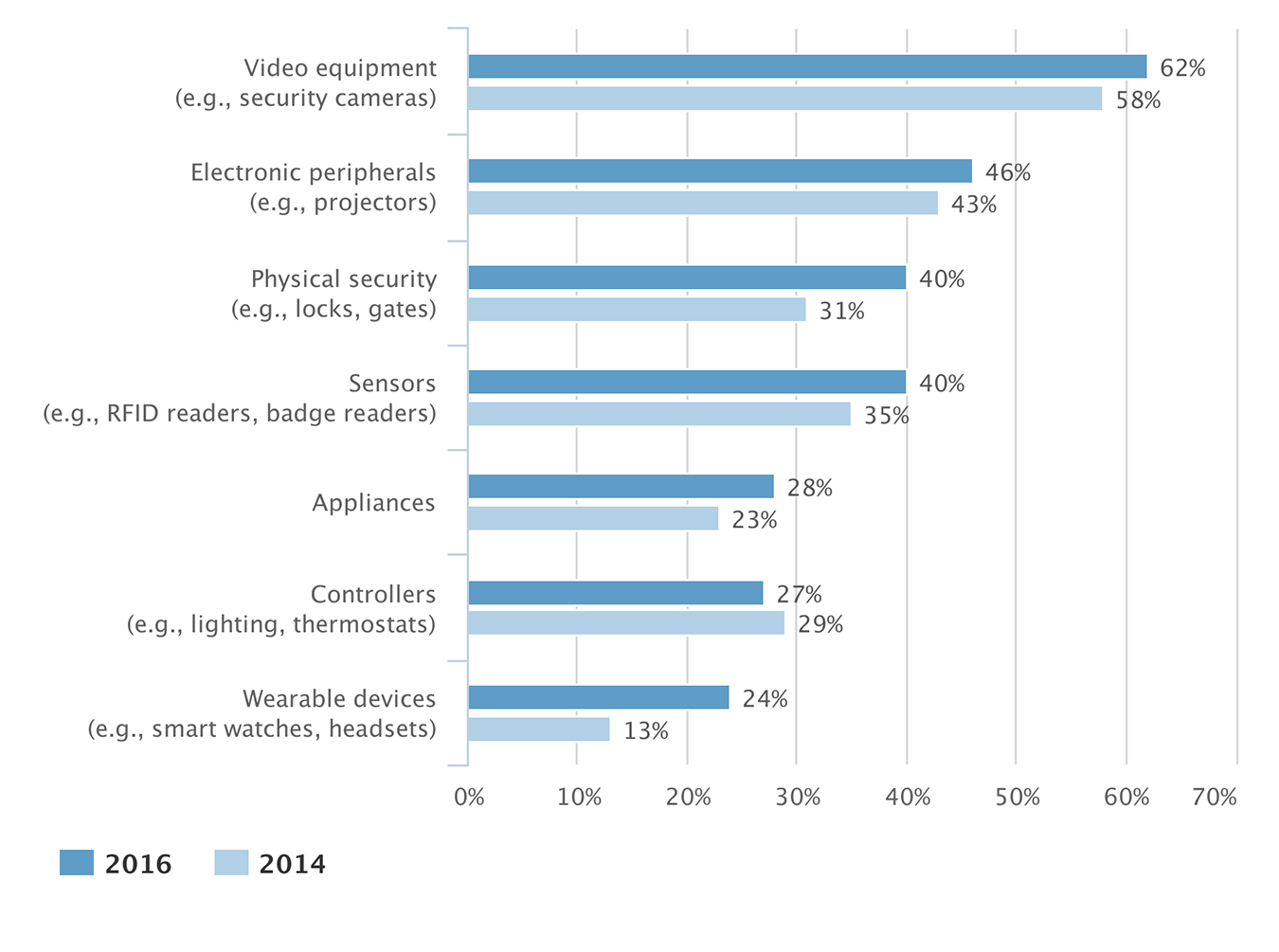
**Figure 2 - Growth in the IoT – Businesses Insider Intelligence ([3], Greenough, 2014)**

Figure 2 depicts the current and future trends IoT market share, this report predicts that by 2019 the overall IoT market will be the largest device market in the world, “more than double the size of the smartphone, PC, tablet, connected car and wearable market combined” reference). This will amount to a predicted $1.7 trillion in value being added to the global economy. This claim is further supported by the global research organization “Gartner Inc.” who also predicts that 25 billion connected things will be in use by the year 2020. Figure 3 displays the predicted amount of smart devices in millions by category;



**Figure 3 – Internet of things units installed base by category**

Although as evidence, the Internet of things promises to effect a range of markets, this investigation will focus mainly on the domestic consumer market. Although the consumer market will not account for most of the revenue that is predicted to be generated by the internet of things, it will be responsible for driving the predicted increase of connected smart devices ([4], Gartner Inc., 2014), The domestic market for smart devices consists of a wide range of devices, figure 4 below from marketing research firm “spiceworks” depicts the range of domestic devices and the percentage of them with “smart” capabilities:



**Figure 4 – Internet Enabled “Things” Connected to Networks (North America, Europe, Middle East and Africa)**

Domestically smart devices can be combined in a household to form what we call a “smart home”. Smart home solutions are becoming ever more popular in the western world with smart devices controlling household heating through smart controllers, lighting through smart lightbulbs, physical security through smart locks, IP security cameras and even personalized shopping lists through smart fridges. As useful and impressive as smart devices seem it is important that we remember to take into consideration the security aspects, just as any other computer system, unauthorized access and usage can compromise devices. In professional networks it is generally considered that the Internet of things, smart homes and smart devices are at risk, more so than conventional computing with a recent BBC article claiming “The smart home, it seems, is pretty dumb when it comes to security.” (reference,).

With the impressive development of the Internet of things and its projected developments for the near future you would assume that a specific focus on security would be at the base of all advancements, however it is feared that in the competitive rush to develop IoT devices developers have not taken security as seriously as they should have. There are a number of instances emerging online detailing the hacking of devices, the most famous of which involved the hacking of a baby monitor in the US [reference] in this case it was claimed that a hacker had access to the video and audio capabilities of the device, which is understandable cause for concern. There is also the recent example of compromised webcams, IP security cameras, digital video recorders and routers being involved in one of the biggest denial of service attacks ever recorded, this particular attack occurred in October 2016 and took popular sites like Reddit, Twitter, Spotify and Tumblr offline [reference]. The use of smart devices in this attack underlines the importance of IoT device security as not only can it be crucial to the protection of users but also organizations worldwide.

The apparent vulnerability of smart devices has been documented in a number of studies, one specific study carried out by Hewlett-Packard declared that “70 percent of internet of things devices are vulnerable to attack” [Reference]. This state of vulnerability is cause for concern to security professionals.

This investigation aims to establish the current state of the Internet of things devices and how it can adversely affect the security of a smart home and its users aiming to educate on what the most popular vulnerabilities of IoT devices are and therefore what countermeasures can be implemented in order to future proof the internet of things as a whole, protecting its users from cyberattacks and cybercriminals.