Greater Manchester | Greater Security | Greater Business

# Cyber Foundry

# The Industrial Internet of Things

## How industry is connected to IoT & cyber security

**Audience: General** **Reading Time: 15 Mins**

*The Internet of Things (IoT) goes beyond smart speakers and home heating. It is revolutionising and enhancing all of industry, from work safety to better logistics and more. In this article we explore the cyber security implications of the Industrial Internet of Things.*

## Key Points

- As microprocessors have rapidly shrank, the Internet of Things has rapidly expanded, allowing almost any device the ability to be connected to the internet and become a 'smart device'.
- Cyber security is often considered as a secondary, or after thought in many production cycles. This is a significant problem which further increases the potential risks from malicious actors
- The implementation of smart devices throughout industry has led to numerous benefits, from improved operation efficiency to better understanding of customer demands.
- IoT devices generally lack direct user interaction. This is increasingly drawing cyber attackers to target IoT devices, as they are less likely to be noticed.

European Union
European Regional Development Fund
The Cyber Foundry project is part funded by the European Regional Development Fund

Lancaster University
MANCHESTER 1824 The University of Manchester
Manchester Metropolitan University
University of Salford MANCHESTER

# Benefits of IIoT

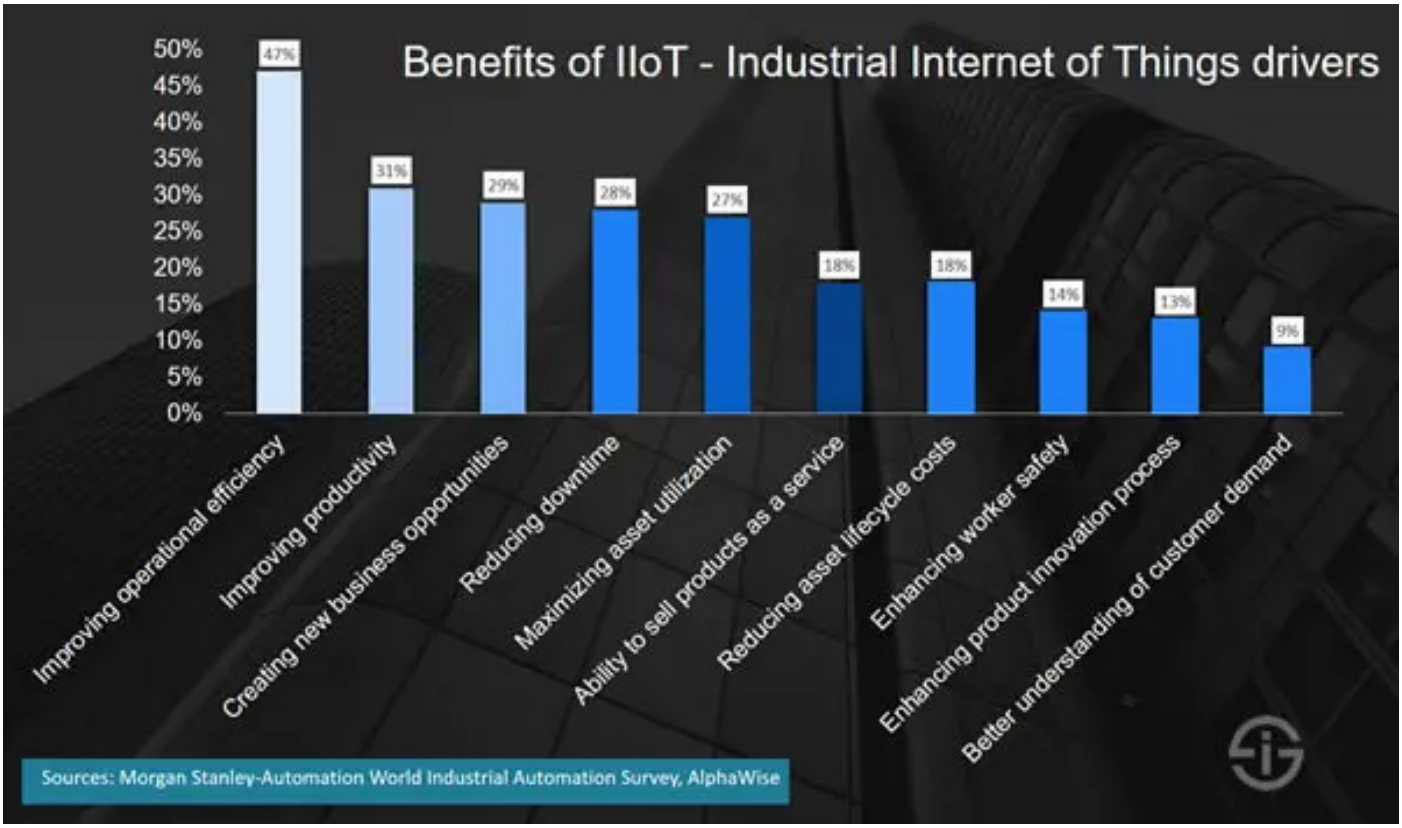
The Internet of Things (IoT) is often referred to as the ever-expanding web of inter-connected devices, comprising of numerous everyday items all connected to the internet (O'Maley, 2016). With consumers being drawn into the technological wave of IoT, the evolution for opportunity is becoming endless, allowing almost any device being able to connect to the internet, with massive amounts of data available for big consumer brands to obtain. This has become possible due to the incorporation of small computer chips that allow you to connect devices to the internet easily and competitively. For around a decade rapid growth as allowed businesses to explore new ideas and interests, modernising everyday technology to automate goods and dramatically change the world.

There are now an extraordinary number of items that come in all shapes and sizes, such as smart fridges, which have interactive notes on the fridge and allow you to access the internet on the fridge door; to smart cars which have complex sensors to detect objects in their path, and sensors in the boot of the car in order to open it via movement or proximity. Almost anything can now be connected to the internet to track data, no matter the size, due to the availability of micro-computer chips. If you wanted to check the time spent brushing your teeth, to the speed you can throw an apple, it is all now possible from the use of sensory equipment and hardware engineering. This article will discuss how IoT is relevant within industry, the cyber security threats that may pose a threat, and the challenges currently faced.

## How Is IoT Relevant Within The Industry?

The *Industrial Internet of Things* (IIoT) opens up opportunities in automation, optimisation, manufacturing, performance management, maintenance, industrial control, customer centric roles and smart industries.

IoT within business, is used for several different motives however, most companies use it to improve operational efficiency and to improve productivity. These smart technology devices which are incorporated help assist businesses to move into a much smarter means of working and streamlining their processes.



# Leading IoT Users

The Internet of things is evidently changing the way people do business as can be seen from the above chart. It is used in various ways however, more importantly to create smarter business models, and streamlining operations to reduce expenditure. With the intelligence enabled through smart devices, it can be programmed to work in unison to produce outputs on an assembly line, and it can collect data on the status of the environment and equipment that allows fail-safes and smart technologies to be put in place that allow proactive maintenance or automated recovery after failures (How IoT will Impact Different Industries, 2020).

Industrial IoT has proven successful in several different sectors from agriculture to manufacturing, in order to assist and enhance the speed and maintainability of their systems. A good example would be engineering firms that need to monitor and maintain equipment, who require an easy way to monitor faults and issues with their hardware. IoT can play a reliable part in streamlining this process and allowing for data to be captured when issues happen and to better understand system failures and workplace faults.

A popular product, which many households now see, related to the Internet of Things are devices such as the *Amazon Echo*, *Apple TV* and many other smart devices that crop up around the house to streamline processes. It is now easy to ask your 'personal assistant' to remind you at a specific time, order a product via speech or even ring someone without needing your mobile phone. These devices are also very common in organisations and offices in order to create smart office environments. The flexibility of IoT technology and how it can be embedded in many different devices, it makes them extremely useful in a wide range of applications and environments. It offers many businesses the opportunity to increase production and automation, along with improving data processing and analytics.

Organisations worldwide have already incorporated and connected technology by embracing industrial IoT projects and using these applications and technology to drive their business forward. According to Buntz (2020) there are several giant companies that embrace IoT such as:

- **Amazon** – Amazon use technology within their warehouses and logistics to improve the way human and machine collaborate. Amazon have Wi-Fi connected Kiva robots within their warehouses that locate the products quickly on the shelves and give them the workers.

- **Bosch** – Bosch has a track and trace innovator to help with an issue they had with workers spending large amounts of time finding equipment. They added sensors to its tools in order to track them.

- **Hitachi** – Hitachi have produced their own IoT-enhanced production model and have slashed production by half for the manufacturing they do with infrastructure.

- **Boeing** – Boeing are making use of IoT to drive manufacturing efficiency. Their technology is driving efficiency throughout factories and supply chains and steadily implemented sensors into their planes.

As you can see from the above examples, companies are providing solutions to their problems within their organisations in order

*image: Alex Gate, Unsplash*

to create technology related solutions, speed up operations and work smarter. Where new technology is being implemented into the workplace and collecting sensitive data ,or making significant impacts to business operations, security is extremely important.Specifically, cyber security is an important factor to consider when looking at implementing any IoT device into the workplace, in order to protect against things such as hi-jacking, distributed denial of service attacks (DDoS) and architecture hijacking, etc.

## Industrial IoT Cyber Security

Analysts predict that by 2025, there will be roughly 21.5 billion IoT devices connected worldwide drastically increasing the surface area for the cyber-attacks (Addressing cybersecurity risk in industrial IoT and OT - Microsoft Security, 2020). Due to this, IoT within industry is now trying to revolutionise the way that they work and manufacture products, as the implications for cyber-attacks can be disastrous and sometimes fatal due to safety failures and loss of life. It is highly important to understand why IoT devices are becoming increasingly attractive targets for hackers, it is due to these malicious actors being relatively unnoticed and undetected from the lack of direct user interaction of IoT devices.

Here are a some more reasons for why these devices are attractive targets for hackers:

- They perform critical functions within the operations of companies which can cause complete chaos and havoc when they are compromised. This may be due to security flaws in industrial equipment that can be hacked and cause production issues.

- They fuel DDoS attacks and disrupt operations due to the scalability of applications on the market. They are always on also, so they are always available to attacks due to their availability.

- Their operating system can play an important role in faciliating attacks, as many use low-cost common code libraries which contain unpatched vulnerabilities and lack basic security due to minimal processing power.

- They have outdated firmware due to the difficulty of maintaining equipment and hardware. Also, using weak authentication methods for user ID and passwords, or lacking them completely.

From the list it is evident, several devices create their own security flaws by not updating software, using correct authentication methods and keeping up to date with library patches. It is of significant importance that IoT standards are implemented and followed along with best practices to reduce security flaws in IoT systems.

*image: Louis Reed, Unsplash*

## Security Challenges

Several recognised risks with IoT are how products are used, what they are used for and how they are maintained, all these factors will determine potential DDoS attacks and exploit vulnerabilities (Lindqvist & Neumann, 2017). The challenges that are posed generally fall down to vulnerable components, increased connectivity, insecure protocols and human error. Most systems are rarely designed with cybersecurity in mind and the vulnerabilities and attacks within software are becoming more and more common. Another intriguing

factor for cyber threat management is prioritising it during process management. Within most hardware development projects the functionality and efficiency are usually prioritised higher than that of cyber security.

Managing IT and IoT integration is a significant challenge, the contributing factors include unsecure network connections along with unknown risks in IoT related environments. Legacy controlled IoT systems again form a solid issue as manufacturers build new systems on top of legacy (i.e. outdated) systems. This compounds the outdated protection measures which maye contain unknown vulnerabilities that have been inactive for years. Human error may fall down to users not being familiar with new processes and systems that are incorporated, which can be the case for email phishing if hardware is sending data via emails.

Device security and maintenance should be a subject of consideration through the product's entire lifecycle up until the product is no longer required or used. System architecture can always be exposed and be vulnerable if cyber security considerations are not maintained, and fixing the threat to the hardware is often at the bottom back of the 'to-do' list. It requires high-level maintenance and uptime monitoring in order to identify any intrusion, corrupt data or security flaws so that all data is securely stored and maintained.

## Cyberattacks on IoT have surged

It is no surprise that IoT vulnerabilities have surged in recent years due to the mass number of connected devices on the market. According to (10 IoT Security Incidents That Make You Feel Less Secure, 2020), there are a number of good examples of prolific vulnerabilities from companies in recent years such as:

- Smart security cameras such as *Amazon's Ring Video Doorbell Pro,* which may have given hackers unauthorised access to the user's WIFI network and to other connected devices on it which received a security patch. Researchers however, found flaws that may allow hackers to view video footage and listen to audio output.

- Smart Televisions have several neglected security issues and, according to the FBI, hackers can control unsecured devices to change channels, adjust the volume and make use of the cameras etc.

- Smart homes can be vulnerable with technical glitches and hacking into the WIFI. A couple in the USA had their smart home compromised where the video system was controlled, and room temperatures were hacked from exploiting the thermostats.

- Smart speakers, fridges and bulbs can be hacked. Researchers have identified ways to access the Amazon Echo smart speaker and attack it with malicious programs. Though Amazon appear to be on top of their security issues and provide patches regularly for any of their flaws.


*image: Dan Lefebvre, Unsplash*

None of this is intended to scare you. Rather, it is to help you understand how anything that has an internet connection can be manipulated and be prone to attack, so it is important to assess the risks and defend against them early on. However, with Industrial IoT, data loss and attacks can be substantially more damaging than a smart home speaker and will pose their own threat depending on the functionality on the IoT device.

# Further Support

## How to defend against IoT cyber threats

There are several scenarios which can cause pandemonium if a hacker took control of your product due to finding security flaws within your systems. Since IoT provides access to real-world objects, then an attack can cause real world harm to people, and even result in loss of life which can completely destroy your business. There are many scenarios that hackers can take control and jeopardise a system such as self-driving cars being hacked, locks in smart home doors being unlocked or manufacturing equipment being hacked and causing faults. This is the main reason security must be at the forefront of any technical project that is connected to the internet. Many think it will not happen to them, or the chance of it happening is too low. However, security should constantly be embedded in every aspect of IoT development.

In order to combat against attacks it is important to consider protecting against physical tempering and keeping hardware out of reach of potential assailants. According to (Elizalde, 2020), a hospital invested millions into cyber security however when a nurse charged her phone a *Trojan horse attack* found its way into the hospital's network, which highlights just how easy it can be to fall foul of cyber attacks. Therefore, it is important for all product managers to ensure cyber security is considered throughout the full life cycle of the application in order to combat any potential future threats.

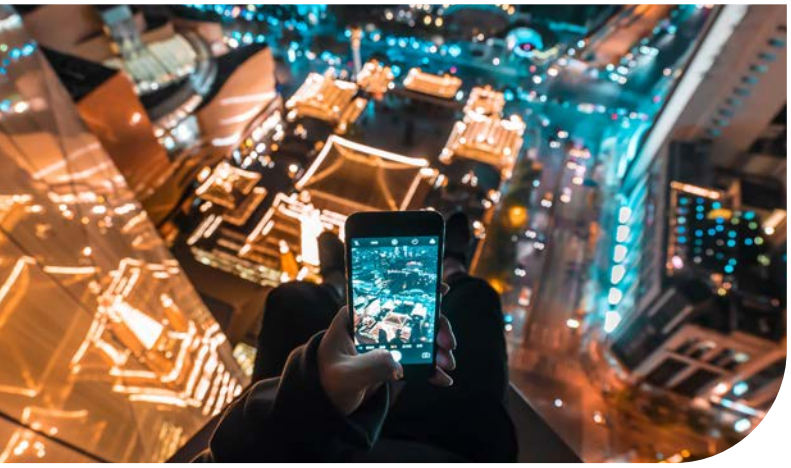


*Image: Yiran Ding / Unsplash*

## Further Support Available

The **Greater Manchester Cyber Foundry** runs a *Secure Digitisation Programme* designed to support businesses facing cyber challenges in the Greater Manchester area. We believe that cyber security is more than just a necessary safety feature anyone using digital technology; cyber security is also a vital driver for innovation and growth in all business.

The programme teaches the basics of secure digitisation before going on to explore how you and your business could grow and thrive through cyber innovation.

The support is free due to being part funded by the **European Regional Development Fund**, and is in partnership with **Lancaster University,** the **University of Manchester, Manchester Metropolitan University,** and **Salford University**.

The programme normally consists of two full-day workshops, alongside some online open learning elements. In addition, enrolling gives you access to our digital portal full of cyber innovation tools and services to better **defend**, **innovate** and **grow** your business. There is also time available to meet 1-to-1 with our business development team who can offer bespoke insight and signposting to the best next steps for your business. This can lead to technical assistance in cyber innovation from a dedicated specialist teams from one of the partnered universities.

To find out more about how your business can access support and register on one of upcoming cohorts contact us:

gmcyberfoundry@lancaster.ac.uk

# Further Reading

**About the Author**

**Dom King** is an Analyst Developer for the Greater Manchester Cyber Foundry project. Having a key interest in human interaction and IoT, he has completed a master's degree in Human Computer Interaction with a project related to navigational systems using Arduino and GPS technology. In his spare time, he runs his own web development business and aspires to create a range of technical podcasts in the future. One of Dom's favourite reads is *Hooked: How to Build Habit-Forming Products* by Nir Eyal, which is a fabulous book on user behaviour.

Lancaster University

## READ MORE


1. Buntz, B., 2020. The Top 20 Industrial Iot Applications. [online] IoT World Today. Available at: <https://www.iotworldtoday.com/2017/09/20/top-20-industrial-iot-applications/> [Accessed 20 September 2017].

2. CISO MAG | Cyber Security Magazine. 2020. 10 Iot Security Incidents That Make You Feel Less Secure. [online] Available at: <https://cisomag.eccouncil.org/10-iot-security-incidents-that-make-you-feel-less-secure/> [Accessed 10 January 2020].

3. Elizalde, D., 2020. How To Protect Your Iot Product From Hackers. [online] Daniel Elizalde. Available at: <https://danielelizalde.com/iot-security-hacks-worst-case-scenario/> [Accessed 28 July 2020].

4. i-SCOOP. 2020. Business Guide To Industrial Iot (Industrial Internet Of Things). [online] Available at: <https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation> [Accessed 10 October 2020].

5. LINDQVIST, U. and NEUMANN, P., 2017. Inside Risks the Future of the Internet of Things. Association for Computing Machinery.Communications of the ACM, 60(2), pp. 26.

6. Machine Design. 2020. How Iot Will Impact Different Industries. [online] Available at: <https://www.machinedesign.com/automation-iiot/article/21836897/how-iot-will-impact-different-industries.> [Accessed 8 March 2019].

7. Microsoft Security. 2020. Addressing Cybersecurity Risk In Industrial Iot And OT - Microsoft Security. [online] Available at: <https://www.microsoft.com/security/blog/2020/10/21/addressing-cybersecurity-risk-in-industrial-iot-and-ot/> [Accessed 21 October 2020].

8. O'MALEY, D., 2016. The Internet of Things. Journal of Democracy, 27(3), pp. 176-178.

9. Securitymagazine.com. 2020. Protecting Distributed Iot Devices. [online] Available at: <https://www.securitymagazine.com/articles/92738-protecting-industrial-iot-devices> [Accessed 2 July 2020].



*For more info about GM Cyber Foundry:* https://www.gmcyberfoundry.ac.uk


European Union
European Regional Development Fund
The Cyber Foundry project is part funded by the European Regional Development Fund

Lancaster University · Manchester 1824 The University of Manchester · Manchester Metropolitan University · University of Salford Manchester