Greater Manchester | Greater Security | Greater Business

# Cyber Foundry

# 8 Cyber Innovation Predictions for 2020

## How your business can navigate them!

**Audience: General** **Reading Time: 10 Mins**

*2019 was an eventful year and the end of an eventful decade for cyber innovations. We predict that the next decade will bring even more disruptions and opportunities. Starting with the encumbent year see below for our eight headline predictions for 2020. Read on for a full comment on each.*

## Key Predictions

- **Prediction 1:** There will be an increase in IoT devices being sold worldwide and an increase in more significant cyber-attacks utilising the immature security of IoT networks.
- **Prediction 2:** The national discussion around truth and trust will continue and be exacerbated by the mainstream introduction of deepfake technologies.
- **Prediction 3:** Data privacy will become a complex legislative and compliance battleground as a consequence of the UK leaving the European Union.
- **Prediction 4:** The value of data will continue to increase. This will build awareness of the importance of data but in parallel the important of cyber security and cyber innovation around data.
- **Prediction 5:** The cyber skills gap will increase and businesses with cyber innovation and cyber security skills within their team will be at an advantage over their competition.
- **Prediction 6:** The hype around blockchain will continue as people start to try and understand the financial applications of the technology. However, we don't think many new blockchain products, services or solutions will be released to the market.
- **Prediction 7:** We predict ransomware will make a more targeted and sophisticated resurgence, and become harder to deal with.
- **Prediction 8:** There will be an increase in sophisticated mobile malware, targeting individuals and businesses for more sophisticated reasons than just theft.

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

# The Asbestos of IT

## 1 - The Internet of Things (IoT) Will Become A More Significant Security Problem

It is predicted that there will be ***20.4 billion IoT devices by 2020***.[1] That is more devices than humans to a nearly 3:1 ratio. Although this is great for technical interconnectivity and cyber innovation, this poses a huge potential cyber security threat. We are currently within the wireless wild west with IoT (comparable to the Internet boom of the 90's).

The *Internet of Things* refers to the ever-growing network of physical objects that feature an **IP address** for Internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems. Examples are: smartphones, Amazon's Alexa, Apple watches, smart TVs, or an intelligent (smart) fridge, etc.

This emergent technology is in its commercial infancy and there are lots of questions surrounding the safeguarding of consumer privacy and the trust of the service providers. Smart devices are currently being sold at an unprecedented rate, which has an impact on the necessary protective laws on things like data protection - i.e. it will take a while before legislation is able to catch up. This means a wireless wild west is being created which is perfect for those with both good and ill intentions to exploit. This is very similar to the timeline of Internet security when the world-wide web started. At its genesis there was no legal or social structure to enforce the limits of the Internet. However, once legislation caught up, frameworks were brought in to facilitate safe passage for consumers being online.

One leading expert Mikko Hyppönen from the company ***F-Secure*** likens IoT and smart devices to the asbestos of the IT world.[2] That is to say that we are filling our environment with a potentially highly dangerous legacy of smart devices which will eventually need to be specially dealt with and removed safely in the future. This is why we advocate for a *secure by design* approach. On a more optimistic note, this also highlights the types of new business opportunities, from electricians to smart home installers or even refurbishers; demonstrating the need for cyber innovative business in the new world of IoT.

## 2 - Information Warfare Will Increase So Will People's Awareness of This Too

The phrase *fake news* was made infamous by President Trump in 2016 and ever since there has been an international debate around how truth is mediated on the Internet. Not only is misinformation distributed inadvertently, but there has been a deliberate step to weaponise false and misleading information, and it is growing rapidly.

In 2018 we saw the fall of ***Cambridge-Analytica.*** A company which many had never even heard of collecting **aggregated data**, suddenly filled the headlines and became world famous for its potentially unethical harvesting of personal data and readiness to sell this data

### Definitions

- **IP Address** - *a unique string of numbers separated by full stops that identifies each digital device.*
- **IoT** - *a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human, or human-to-computer interaction.*
- **Aggregated data** - *The collection of small seemingly valueless pieces of data which together create a valuable data set.*

as a political weapon. A question which was asked of the time but is still relevant in 2020 is: *How many other Cambridge-Analyticas are there?* With the increased value in aggregated data, it is hard to imagine that Cambridge-Analytica is the only company skirting the moral boundaries of how aggregated data should be used in society.

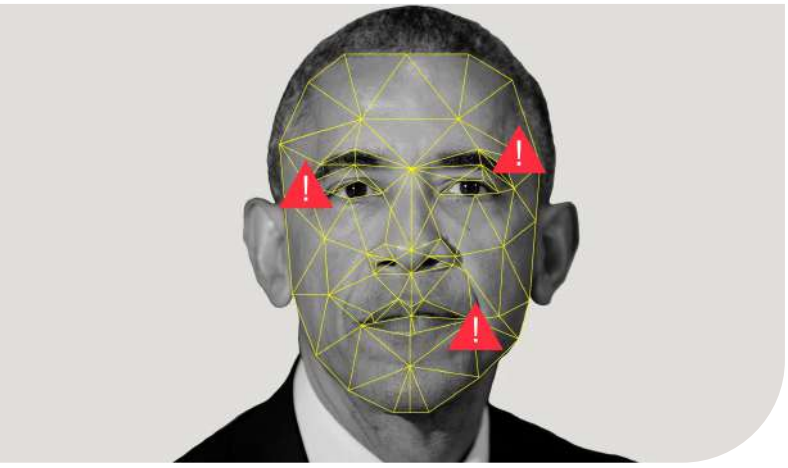


*Image: Alyssa Foote; Olivier Douliery/Getty Images*

As social media intelligence (SOCMINT) has become more video based, so have the weaponised techniques of misinformation. This married with the significant step forwards in artificial intelligence (A.I.) we predict to see an increase the rise of *deepfakes*.

Deepfakes are an artificial intelligence technology which alters the content of a video to misrepresent something that did not actually occur. Originally used in pornographic videos in 2017 to replace the faces of adult film stars with the faces of mainstream actresses, the technology has recently started to be demonstrated on more significant figures such as celebrities and world leaders.[3] Although at the time of writing there have been no direct cases recorded of it being used for political gain, it seems almost inevitable that this will feed into the dialogue around truth, trust and the Internet.

Mediating truth used to be the purview of the mainstream press, but the democratisation of *publication* has not seen a similar democratisation of *mediation and fact checking*, specifically about the individual - ***You***. This gives rise to abundant business opportunities to help manage this deluge of content and information, from automated processes to fact check social media; to systems which ensure your personal data is accurate and is only as public as you are happy to allow.

### 3 - Brexit Could Lead to Greater Government Data Governance, or Less - We Are Not Sure!

Since the 2016 referendum, the UK has been negotiating its new relationship with the Europen Union. Whilst the subject of Brexit and what will or will not happen has been a constant, one particular aspect you are unlikely to read about in the media is the the potential new approach to data law. With the UK leaving the EU this could give greater power to the UK government surrounding data governance and regulations.

> *deepfakes will feed into the the dialogue around truth, trust and the Internet*

Potentially, this may see substantial changes to the UK's *Data Protection Act 2018* which enshrines the EU's *General Data Protection Regulation (GDPR)* into UK law. Currently the GDPR states that you need to enforce this regulation if you are a *controller* or a *processor* of personal data taking place in the EU; or if you are controlling or processing data of EU citizens, regardless of whether your organisation is in the EU or not.

There are three possible outcomes:

**1)** The government maintains UK law such that there is regulatory alignment with the EU.
**2)** The UK increases consumer protections exceeding and encompassing EU regulations
**3)** The UK decreases consumer protections, falling short of the EU regulations

The first one represents business as usual, the second and third positions represent additional implications for business. In the second scenario companies will need to put more privacy controls in place; whereas in the

> *In 2017 data overtook oil as the most valuable commodity*

third scenario companies may need to run two regulatory systems - both will result in more red tape for business owners. Regardless of which outcome we see, the concept of *data privacy* is now firmly embedded in to the consumer consciousness and they will expect their personal data to continue to be protected, or they will start shifting to alternate suppliers.

### 4 - Value of Data Will Increase, Therefore So Will The Value of Data Security

In 2017 *data* overtook *oil* as the most valuable commodity[4] and the value of data is still increasing. However, unlike oil whose value increases due to its scarcity of suppy; the value of data is dependent on its volume - the more data you have, the better the data set is. Data is constantly being created and collected, with technology continuing to improve at storing it. Add to this the demand for the ability to analyse and interpret data showing no signs of stopping, we predict the value of data will only increase alongside the demand to ensure the data is secure. The need to handle a wide range of data for the majority of companies, big and small, provides a fertile ground for the provision of new software and professional services. Cyber innovations will lead to *data protection as a service* offerings, or cutting edge cyber risk management approaches to handling business and personal data.

### 5 - The Cyber Security Skills Gap Will Increase

In December 2018, the UK government released their research findings on the UK cyber security skills labour market. They discovered that of the 1.32 million UK business' around 710,000 have a basic technical cyber skills gaps and 407,000 have a high-level technical cyber skills gap.

It also found that 47% of all UK businesses were not confident in dealing with a cyber security breach or attack and 51% were not confident in writing an incident response plan.

*Image: Funky Focus / Pixabay*

Only 14% of organisations have cyber security written formally into a job description. If you combine this, with the increased value of data and the increased number of cyber-attacks, this can potentially spell huge problems for UK businesses.

In the meantime, seek out sound advice from the NCSC [5] or find an approved Cyber Essentials organisation to help you get up to speed on the fundamentals of good cyber security practice.[6]

### 6 - People Will Talk a Lot About Blockchain, But Still Nothing Will Come of It

Blockchain technology has been around a long time, though it is most famously known through its use for the cryptocurrency ***Bitcoin***. Although hitting its peak value in 2018, *Bitcoin* has dominated the **fintech** news headlines of 2019. However, when you read past the headlines, there is not much information there. Much of the hype around **blockchain** technology is simply that, hype. There has been a lot of promise of the potential of blockchain, but we are yet to see this technology become ubiquitous in our lives with a lack of general understanding and regulatory complexity cited as just some of the barriers to widespread uptake.[7]

The concept, broken down very simply, is that blockchain democratises the concept of trust. Rather than trusting one individual with the responsibility of ensuring the integrity of data, you hold a group accountable for verification. The assumption being whilst you may be able to manipulate a minority of agents to you can trust the majority as only a minority would want to consistently lie for their own gain.

Blockchain is often compared in its significance and potential with the advent of the Internet. However, unlike the Internet which was able to be used to solve a very diverse range of problems, blockchain technology is only able to solve a very specific and niche set of problems.

To learn more about blockchain and its potential uses in business, you can read our article on the subject by following this link **here**[8]

Regardless of the utility of Blockchain, Fintech is here to stay. In a world full of digital money - even the GBP is digital these days - there are new finanical service offerings in development, from new banks to open access banking **APIs**. This provides a significantly rich business environment which fundamentally has to be secure and protected. Cyber innovations will drive the growth of fintech enabling greater personal financial flexibility, after all is was only about 15 years ago you had to go into a bank to transfer money to your friend!

### 7 - Ransomware Will Become More Sophisticated and Targeted

**Ransomware** has been a large-scale problem of the last couple of years with high profile attacks like **WannaCry** & **NotPetya** (2017) and **Ryuk** (2018-2019). However, in 2019 the number of ransomware encounters has decreased according the Microsoft security intelligence report.[9] This does not mean the impact on businesses has been any less. What we have seen is people becoming wise

**Definitions**

- **API** - *Application Programming Interface (API) is a software-to-software interface which allows applications talk to each other without any need for user knowledge or intervention.*
- **Fintech** - *Computer programs and other technology used to support or enable banking and financial services.*
- **Blockchain** - *A system in which a record of transactions made in a cryptocurrency (e.g. Bitcoin, or Etherium etc.) are maintained across several computers that are linked in a peer-to-peer network.*

to the simple **spray and pray** techniques of spamming out emails to deliver ransomware, reducing the number of those that are susceptible.

If we follow the trends in other forms of malicious cyber activity, the scattergun approach of mass targeting gives way to more targeted, higher impact attacks; consider the transition from **phishing** to **spear phishing** and now **whaling**. As a result, we believe that over the next couple of years ransomware will become more sophisticated and impactful.

For more information on how to deal with ransomware look at the NCSC guidance.[10]

### 8 - Smartphones Will Become The New Way Into Your Organisation.

Fake app detections are steadily on the rise [11] with Checkpoint reporting a 50% increase in mobile banking malware by mid-2019 compared to the same time in 2018.[12] The target as always is to steal credentials to perpetrate fraud in some way. With predictions there will be 6.1 billion smartphone users by 2020 [13] it is not hard to see why criminals see this as a target rich environment.

The hazard for businesses is that personal use devices are connected to corporate networks to allow their employees WIFI access. This provides an untamed backdoor into the corporate networks. For many small businesses there is no clear delineation between what a *personal* device and a *corporate* device is. While the whole concept of Bring Your Own Device (BYOD) has been troubling security experts for a while, it is the increased focus of criminal activity on the smartphone market which is increasing that concern more rapidly. Combine this with our previous prediction and you have the potential for mobile ransomware; could you or your business survive without access to your smartphone?
Large technology providers have yet to crack the mainstream market with a solution which has seen mass adoption. This gives rise to the potential for an agile, cyber innovative company to corner the market.

The NCSC has published some useful guidance around the topic of security and BYOD.[14]

#### Definitions

- **Ransomware** - A form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment. Users are shown instructions for how to pay a fee to get the decryption key.
- **Spray and Pray** - A derisive term for firing indiscriminately towards an enemy in long bursts, without making an effort to line up each shot or burst of shots, in the hope that at least one shot will land on target and get a result. This is especially prevalent amongst those without the benefit of proper training.
- **Phishing** - The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
- **Spear Phishing** - The fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.
- **Whaling** - Used to describe a phishing attack that is specifically aimed at wealthy, powerful, or prominent individuals. Because of their status, if such a user becomes the victim of a phishing attack, he can be considered a ***big phish***, or, alternately, a ***whale***.

# Support Is Available

## How Can Your Business Navigate The Cyber Challenges Of 2020?

The **Greater Manchester Cyber Foundry** runs a *Secure Digitisation Programme* designed to support businesses facing cyber challenges in the Greater Manchester. As part of this programme there is a workshop dedicated to evaluation of the driving forces which will shape the world of 2020 and beyond. Consider how your business is affected by external changes, now consider how much time your business spends evaluating them and planning for them.

*Image: Yiran Ding / Unsplash*

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. Modules include:

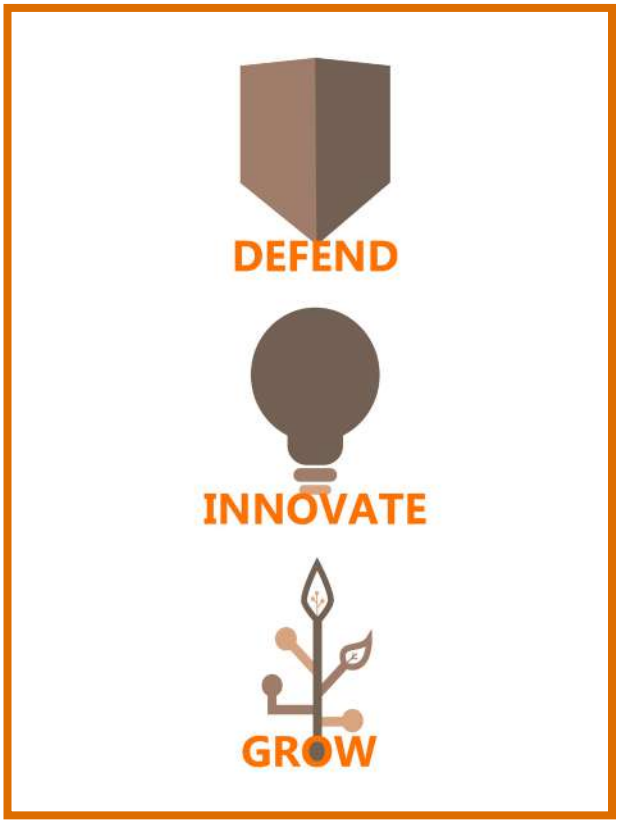
- **Cyber Security Basics** – Baseline cyber security knowledge aligned to UK government standards
- **Cyber Innovation Planning** – Understand how and where cyber innovation fits with your business model
- **Innovation Analysis** – Understanding what innovation is and identifying your company's capacity to act on its strengths
- **Cyber Strategising** – Thinking about the future and where your business may move to
- **Developing a Plan** – Developing an action plan to grow your business

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 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 a bespoke technical assist in cyber innovation from one of our dedicated technical teams from a partner university.

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 Authors

**Geraint Harries** is a technical manager on the Greater Manchester Cyber Foundry project. Before starting at Lancaster University over 2 years ago, Geraint had worked in software development roles in both IBM and the Civil Service. In addition to being a qualified teacher, Geraint has worked freelance with a varied client base as a software developer and graphic designer.

**Dr Daniel Prince** is a Senior Lecturer in Security and Protection Science at Lancaster University. He specialises in Cyber Risk Management and Network Security in complex socio-technical systems, particular cyber physical systems and the financial services sector. He also works closely with organisations to help them understand the economic growth potential of cyber security.

Lancaster University

## READ MORE


1. https://www.vxchnge.com/blog/iot-statistics
2. https://www.verdict.co.uk/mikko-hypponen-smart-devices-it-asbestos/
3. https://www.youtube.com/watch?v=g5wLaJYBAm4
4. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
5. https://www.ncsc.gov.uk/collection/small-business-guide
6. https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body
7. https://www.microsoft.com/en-gb/security/operations/security-intelligence-report
8. https://www.ey.com/en_gl/news/2018/06/regulatory-complexity-is-the-greatest-barrier-to-widespread
9. https://www.lancaster.ac.uk/security-lancaster/cyber-foundry/resources/#d.en.436047
10. https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware
11. https://www.cbronline.com/news/smartphone-malware-mcafee
12. https://pages.checkpoint.com/cyber-attack-2019-trends.html
13. https://techcrunch.com/2015/06/02/6-1b-smartphone-users-globally-by-2020-overtaking-basic-fixed-phone-subscriptions
14. https://www.ncsc.gov.uk/guidance/byod-executive-summary



*For more info about GM Cyber Foundry:* https://www.lancaster.ac.uk/security-lancaster/cyber-foundry/


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