Cyber Security Data Analytics Policy Briefing

Background

Cyber security has come to the forefront of public attention relatively recently, when rising numbers of cyber-attacks, such as data theft, large scale bot attacks and attacks by ransomware on companies and public institutions were recorded. The most prominent of these was the global cyber-attack using the 'WannaCry' ransomware virus in May 2017. 'WannaCry' is particularly threatening as it combines two types of malware: one is a worm intended to spread from one infected device to another, as well as an encryption system rendering data inaccessible for the user.

In the UK, this criminal act caused major disruption to the digital infrastructure of the NHS, which in turn affected the ability of NHS staff to look after patients. While the PM could assure the public that no patient data was lost, this cannot be taken for granted in the future. In the wake of this and many other similar attacks, questions about how cyber security can be improved. The ensuing debate should focus on the following aspects:

- Liability for data theft: current vs. desirable rules
- How to improve security of public service digital infrastructure
- Product regulatory approaches
- Economic incentives for software developers to take cyber security seriously
- Encryption: solution or government dilemma?
- Technical solutions

Problems

The case of the 'WannaCry' ransomware attack highlighted a key issue surrounding cyber security, namely the **availability of malware** on the internet. While at some point in the foggy past a criminal needed to have the ability to write code, this is no longer necessary. Ransomware similar to 'WannaCry' can be bought online, complete with technical support to execute the attack. Similarly, large Botnets can be rented by the hour and utilised in cyber-attacks. Botnets are directed using software such as Mirai, which links together extensive networks of compromised computers and directs them to flood websites with traffic and causing them to collapse. The economic damage inflicted by taking websites offline for significant periods can be potentially huge, as demonstrated by 'WannaCry', when it knocked Telefonica, Deutsche Bahn and many others world-wide offline on Friday, 12th May 2017. Governments are now starting to wake up to the potential for large-scale damage to economies from cyber-attacks on critical industries and infrastructure.

Another problem for cyber security is intimately linked to **the way software is developed**. In a high octane, hyper-competitive environment, software developers are under enormous pressure to release their programmes first to corner the market. Unfortunately, security features within the software are not easily visible and remain in the background- until the software comes under attack. This leads many companies at the cutting edge of software development to 'move fast and break

things', worrying about security features later, if at all. According to research conducted in 2015, an average phone app had 14 vulnerabilities through which malware could be introduced.

Another aspect featuring in the attack was **digital infrastructure**. Although it is difficult to generalise, older and outdated operating systems are often more vulnerable to cyber-attacks than their more contemporary peers. This led Microsoft to the unusual step of issuing security patches for Windows XP, which it 'retired' several years previously. Public institutions in particular often take an 'if it isn't broken, don't fix it' approach to their digital infrastructure, in part due to the enormous costs associated with upgrading the IT systems of large organisations, such as government agencies, the NHS, or Councils.

This weakness can be further augmented by **human error**. It often only takes one click on a link to open malware, thereby compromising an entire system. The larger the organisation is, the greater its vulnerability to human error. In the aftermath of the attack on the NHS, it became apparent that budgetary cuts to the maintenance of the XP operating system have magnified the problem. According to NHS digital, about 5% of devices in the NHS are currently still operating XP. However, these operating systems were the most vulnerable to attack. The fragmented nature of the NHS trust system meant that best practice for digital security was not effectively shared across the NHS.

Advances in chip technology have made them ever smaller and cheaper. **The Internet of Things (IOT)** means that increasing numbers of everyday objects now contain miniature computers, which are connected to one's phone or laptop via apps. Through this interconnectedness, devices become more vulnerable to attacks as the hackers' chances of discovering vulnerabilities increases. Once such vulnerability has been discovered and exploited, malware introduced to the system can spread faster and further thanks to this interconnectedness. The IOT forces us to broaden our focus away from only core devices to every chain in the link.

Additionally, larger machines routinely feature a vast multitude of computerized elements. This means that vehicles for instance feature often hundreds or thousands of computer chips. These are usually produced by different companies and assembled by yet another company, making it near impossible to standardise security features. Often one component in the entire system suffices to gain access. Additionally, the utilisation of computer chips in everyday objects and consumer goods increases the number of potential targets. Hacking software can target these to create botnets.

Companies developing software are faced with an **economic incentive structure** that does not reward investment in digital security measures. Internationally, software companies have successfully challenged their liability in cases where software malfunctioned or was compromised by hackers. In the absence of legal accountability, software developers are unlikely to invest substantially in making their products less susceptible to hacking.

When it comes to correcting this market failure caused by adverse economic incentive structures through **legislation**, governments across the globe have been ambivalent at best. Governments are faced with a classic conflict of interest: they could force companies to comply with higher cyber security standards through encryption, for instance. However, there are also national security considerations at play. It is impossible to make better encryption only selectively available, therefore

any government may opt for higher standards for cyber security. Such a course of action also diminishes the value of such devices as surveillance tools. The alternative option would be to push for lowered encryption standards, as has indeed happened in the past, in which case citizens, companies and institutions become more vulnerable.

Troubleshooting the 'Bugs'

It is easy to focus on the gloomy side of data security by pointing to structural issues which are unlikely to go away any time soon. However, it is more fruitful to regard the increase in cyber-attacks as a positive trigger to review past practices. This section will now provide an outline of potential solutions to address some of the problems outlined above.

There are numerous technological solutions designed to make devices safer and more resilient to cyber-attacks. One of these approaches is 'sandboxing'. The term refers to a system in which individual elements of software are insulated from one another in order to protect them against malware. Researchers led by Dr. Watson, a Senior Lecturer in security, networks and computer architecture at the University of Cambridge, are currently developing ways to implant these sandboxes directly on hardware, thereby avoiding performance penalties associated with sandboxes inscribed in software. The program is called CHERI and funded largely by the US Defence Advanced Research Projects Agency (DARPA), the same agency that played a vital role in the development of the internet.

So called 'formal methods' test small pieces of software using mathematical logic theorems to ascertain whether they execute the functions they are meant to. Recent advances in computing power meant that the technology could make testing of entire programmes commercially viable in the near future.

A market-based solution could centre on the emergence of a cyber security market. Still in its infancy, a fully matured insurance market for digital breaches could incentivise companies to augment their digital security protocols in order to avoid increases of their insurance premiums caused by repeated hacks or data thefts.

Another approach available to legislators would be to force software developers and affected companies to publish any breaches to their cyber security. Current legislation in the UK and US does not require software developers or the firms using this software to publish or acknowledge when they have been breached. In this way, pressure on serial victims could be created to review their security protocols. Governments could also review laws to place liability for hacked or corrupted software or devices squarely and unequivocally on the manufacturers. This would provide a strong financial incentive to make cyber security a priority.