appg **APPG ON CYBER SECURITY MEETING ON CYBER SECURITY**

Date: 23rd June 2020

Present:

Chair: Simon Fell MP

Lord Arbuthnot of Erdrom, Admiral Lord West of Spithead – APPG Officers

Prof Keith Mayes – Speaker

Andre Turville

Scott Petty

Lord King, Marcus Fysh MP. Baroness Finlay of Llandaff, Prof Keith Mayes, Andrew Henderson,

Apologies:

Introduction: Simon Fell MP introduced the topic and welcomed Parliamentarians and visitors. High risk vendors entering the telecoms networks. Less understood is the softer influence through academia and the supply chain.

Presentation

Professor Keith Mayes began with a background summary to the topic area, noting the important work carried out by DCMS and NCSC relating to telecommunications security, SCM and the use of High Risk Vendors (HRV). The roll-out of 5G has driven the pace and urgency for security safeguards; and three areas were described that justified the high priority given to 5G security.

1) Internet of Things (IoT): 5G is not just about people communicating with others, it also includes and enables IoT; where enormous numbers of diverse devices will communicate with other such devices. The anticipated ubiquity of IoT systems and services, and reliance on wireless communications will make 5G a super-critical infrastructure; and any problems of security, reliability or supply could have massive impact on the UK.

2) Virtualisation/Implementation: The core infrastructure of telecommunications networks was once formed of specialist fixed-function computers within isolated and security controlled environments. Within 5G it will be the norm for these fixed functions to become software programmes running on a server; along with many other applications. The function separation and protection becomes the responsibility of the server's virtualisation system. An analogy was given, with the old functions in separate boxes within a detached and secured house, and the new functions in flats within a tower block. Is the block (the virtualisation system) well designed, so that you cannot break into a function to steal, modify or observe; and that information does not leak through the walls to your neighbours? Virtualisation has many practical benefits, but it presents a target for attacks.

3) Embedded SIM (eSIM): Current we use physical removable SIM cards that include a security chip, which has been securely configured by the network operator. Changing phone means moving your SIM; changing network means replacing it. Physical SIMs have underpinned security for many years, but are not suited to IoT where there may be small, inaccessible devices working in harsh

environments. In eSIM (which is being used for SmartPhones as well as IoT) the security chip is embedded in the device and configured later based on a remote provisioning standard that was created by the GSM Association (GSMA). The architecture includes a new trusted third party/managed service provider (MSP) working between the operators and the secure chip suppliers, so that devices can be securely configured for particular networks. We note that in 2018 a hacker group, linked to the Chinese state, specifically targeted MSPs. Although this was not eSIM related it is a warning that these news systems will be attack targets; and require appropriate protection.

In earlier discussions of this APPG, we heard that Huawei, as a HRV, cannot supply core 5G infrastructure, but may be used for radio equipment at the edge of the network. This does not mean that the radio equipment cannot cause mischief (although harder work than the core); and so a network may only use one HRV with no more than 35% of the deployed infrastructure. Potential mischief could include, eavesdropping, espionage, IP theft, tracking of individuals, or simply network disruption.

In 2010 the Huawei Cyber Security Evaluation Centre was set-up, with the goal to provide assurance that Huawei equipment was reliable, secure and safe to use in the UK. However, the centre has not met this goal and casts doubt over the company's processes, which might be a way of hiding unwanted functionality.

DCMS has proposed a new National Telecoms Lab. The intention is to include a mock-up of the UK deployed infrastructure. It needs to be a secure facility, as it will include company IP and may have information about security vulnerabilities that have yet to be fixed or disclosed; which makes it an interesting target for attack. The intention is that the facility is legitimately accessible to government, industry corporates, SMEs and academia.

Academia: Over the past few years, NCSC has done a good job stimulating cyber security activity in academia, and certifying institutions for their research and teaching. The feeling is that academia is meant to be part of the national security solution; with expert resources for training, strategy and help in a crisis. Last year the Daily Telegraph ran a story identifying 20 UK academic institutions (including those certified by NCSC), which received sponsorship form Huawei. The general tone of the article was negative. Oxford University stepped forward and said that they would not take Huawei funding in the future. However, in May 2020 The Register reported £5m of investment from Huawei for Imperial College, related to 5G and AI. We have a confusing situation, with two conflicting examples of behaviour, and no clear government guidance around such funding and seemingly no penalties. What will happen if a Chinese sponsored, NCSC-certified institution, turns up at the National Telecoms Lab and asks for security access?. This is part of a bigger issue. If you put up barriers to direct involvement for HRVs, they will look for access/influence by other means, such as investing in the expertise supply chain, and of course the normal SCM, which will be addressed by other speakers.

Andre Turville

What we have seen from Covid-19 is that supply chains are not inherently resilient. In January the WEF produced a report on short term business risk and the underlying supply chains. This covered climate change, geopolitical and cyber attacks, at the time there was no mention of Pandemic. What Covid has done is increase the risk of Geopolitical (economic nationalism) and Cyber risk. As an example PPE has shown us that we have insufficient visibility of supply chain and the risks, in turn crisis management. The same response and challenge remains if hit by a cyber attack or geopolitical event. We have adapted how we do business during Covid, increasing our digital footprint, how we communicate, share as we work from home which means more attack vectors, this has seen an exponential increase in attacks since March – an example of how attackers take advantage of weakness in the chain.

Attending a previous APPG meeting came to three conclusions about cyber risk in the context of business risk and that of critical national infrastructure:

1) Understanding that IT depts alone should not be in charge of cyber risk as they do not understand risk in the full business context (c-suite responsibility). Hackers become more sophisticated and look for weaker links in supply chain as corporates are able to spend money on defences (fortress approach) but SMEs are not and lack expertise, they are attacked to disrupt the whole value chain creating asymmetric attacks on larger organisations. State actors, organised crime, industrial espionage, terror or activists taking the same approach.

2) There is the human factor which is hard to manage, as much 90% of attacks have been recorded to have some human element, controls need to be tighter and increased level of learning at the individual level. The final point is access, the bad actor will go for the weakest link, the person or organisiation that has low cyber maturity and understanding.

3) Scale – greater interconnectivity means we are only as strong as the weakest link, typically smaller organisations do not have the cyber maturity, security or funding to protect themselves. They need to be supported for the health of the whole supply chain, with affordable tools to manage their cyber exposure and adherence to standards and legislation.

65% of firms surveyed by Hiscox reported that they had been victims of a cyber attack. Post Covid, expects a closer look and re-drawing of supply chains, more near or on-shoring of supply chain, this presents an opportunity to build more robustness. Standards and controls are not global and are interpreted differently. The scale issue is about resources and tools, how do we enable organisations to manage risk properly and harmonise controls and standards?

Key points

Cyber criminals are using weak links in supply chain to make targeted attacks

Lack of visibility of supply chain visibility creates significant business risk blind spots

Cyber risk can no longer be the sole domain of the IT department – Board accountability

Greater digital interdependency & IoT exponential growth in attack vectors

Multiple international standards cause confusion and liability

Resilience is key and better oversight is needed for supply chains. Need to understand the supply chain and the maturity of cyber security in the different elements. Large corporates are usually well served but not the SME and smaller firms lower down the chain need to be supported to ensure the integrity of the whole value chain.

Scott Petty – Introduced Vodafone as a company.

Take a multi-layered approach to security and the UK is home to Vodafone's global cyber defence capabilities. Work closely with NCSC. All vendors equipment and service are potential risk factors. Minimise outsourcing to ensure control. Do use Huawei for base stations (18000 base stations in the UK). The IP Security gateway is the most important base station element as it controls access to the network and Vodafone do not use Huawei or any risky vendors for this component. Under 5G security is further enhanced as data is encrypted.

Welcome the DCMS review and the 35% cap on risky vendors. Enables Vodafone to maintain resilience. Would like further diversity as limited to Ericsson, Nokia Siemens and Huawei. Testing the technology in rural areas first to ensure coverage.

Mobile is a heavily standards based industry. These are made by the vendors (including Huawei, Ericsson and Nokia Siemens), mobile operators (including the Chinese ones such as China Mobile). Chipset manufacturers (Qualcom and Arm). This enables interoperability across the network. It also creates scale, 4G has seen most of the world using the same technology and standards. It creates lower price points and a larger market for the manufacturers which leads to lower pricing, better handset development etc. As a result the scale that is create means that lower prices can be offered. The 35% threshold means that Huawei gets enough access to continue to develop standards etc.

As those vendors contribute to standards they reach out to academia on a global basis and fund universities to try and get a leading position in the market. Huawei, Ericsson, Nokia etc. all do this.

Ericsson and Huawei are similar in terms of feature sets with Nokia lagging behind. Others are working to catch up like Samsung.

Questions

1 – MW – how can we collate lessons from Covid-19 to identify them and put the learning into practice?

AT – there is a lot to be learnt. Covid has demonstrated a woeful lack of understanding what supply chains look like. Specifically a lack of skill sets and situational awareness. More concerned with government level effects, how the Chinese or US will do business with the world than with particular companies.

SP – Telecoms networks have performed well. Started to order PPE back in January as Vodafone saw the pandemic develop as they were able to track other markets in which they operate. Lesson learnt is paying attention to the supply chain. Do have some exposure, 80% of the worlds optic connectors are produced in Hubei province so how does one avoid dependencies on suppliers.

KM – Running a crisis exercise could be a good way to think about how to best engage academic institutions and their staff; who could the government call and trust? A crisis event might also highlight contractual risks where large companies sub-contract their risks to smaller companies. Recall the banking crisis in which risk was passed through the supply chain and the little guys could not cope; is it the same with cyber security?

2 – FY – what process does Vodafone have in place to vet manufacturers.

Full supply chain management process and work with NCSC on this. New equipment is much lower risk than old equipment and processes. Part of the challenge is managing the life cycle of old equipment and ensuring that it is patched and up to date. Do not invest enough nationally in lifecycle management. We expose ourselves to greater risk by elongating the lifespan of equipment.

3 – Baroness Finlay – concerned about the app developed by NHSX. How can we, as Parliamentarians, make sure that the governance processes behind decisions are properly made? Would like to understand governance process better?

SP – NCSC published detailed architecture diagrams for the app which was good in enabling understanding. NCSC works closely with industry to develop cyber security standards and share intelligence. This is lacking in many other markets.

KM – There was a letter signed by 100s of UK cyber security academics raising concerns about the original app. Consensus was that due to the crisis (and best intentions) the app was being rushed out without enough attention to data privacy. The risk was not necessarily from the intended legitimate use, but from attackers.

Baroness Finlay – understood that app was developed with security input?

KM – Security experts from the NCSC will have been involved, however security is always a compromise based on the risk situation. Perhaps saving lives was deemed to outweigh the privacy risks, and it took time to determine that the less centralised solutions had reduced risks. There have been suggestions that all these apps might not work too well, as many people turn Bluetooth off to save battery life.

Baroness Finlay has real concerns about access to data.

4 – Lord West – initially we were content that we were monitoring Huawei, only the last three years that concerns have really been made public. Do we want China deeply embedded in a whole raft of areas of our national life. Ericsson is vulnerable as well.

Almost like back in 1945 when we had helped the US develop the atomic bomb and had to go down our own route ourselves at huge cost to build a British bomb. It would be worth the UK doing the same.

SMEs in the supply chain are a worry. Dreadnought submarines are an example with small suppliers producing important parts.

AT – traceability is really important to find out who made a small component. When you start to look at the where the weak links are e.g. using a florist to gain access to a building.. Worth the investment and pain to trace parts.

SP - UK become a significant player in Open RAN (Open Radio Access Network (O-RAN) technology Likelihood that we could catch up with existing technology is hard to believe though.

5 – Keith Mayes – as the network ages, there are many Chinese handsets in circulation and the number is rising worldwide. Does Vodafone have concerns about the rise of Chinese handsets.

SP - Huawei has 7% market share. Other Chinese vendors use Android and need non-Chinese chipsets. If the chipset were manufactured in China it would become more difficult. Risk would increase, but currently Chinese vendors have a very small UK market share.

Simon Fell concluded by thanking the speakers for their time. Will send follow up letters to Ministers, copies will be sent round.