APPG ON CYBER SECURITY MEETING ON THE CYBERSECURITY AND RESILIENCE BILL, 11TH DECEMBER 2024 AT 3.00 P.M. ROOM W2

Title: The purpose of the meeting is to generate ideas for inclusion in the forthcoming Cyber Security and Resilience Bill.

Chairman's welcome
Apologies: Lord West, Lord Mackenzie, Lord Sharpe, Kit Malthouse MP (APPG Chair)
Present: Lord Arbuthnot (Chair), Lord Hogan-Howe, Baroness Neville-Jones
Andrew Henderson (secretariat); Dominic Connor; Glen Bluff; Freha Arshad, Accenture; David Cook, DLA Piper; Prof Ian Philips, Loughborough University; Andrew Churchill and Adrian Jolly, IoCR; Chris Jamieson and John Poon, Novacoast; Kuan Hon; Gerard Philips; Carla Baker, Palo Alto; Charles Wynne, Lloyds of London; Julia McCarron and Ellis Hurst, Advent IM; Philip and Arthur Virgo, House of Lords; Luke Barton, Comptia; Ollie Buckley, TASO Advisory; Steve Penny, SANS Institute; Steward Room, DWF Law.

Speakers:

a) **Andrew Churchill, Institute of Corporate Resilience** – *Lead on the original Home Office Cyber Crime Task Force (2000-2001), and subsequent research for Government and industry into vulnerabilities in, attacks against, and defences for Identity & Authentication technologies/ techniques. Led the Open Banking wargaming exercises and lead author of the British Standard in Digital Identification and Strong Customer Authentication, UK lead on International Standards Organisation on e-Commerce Transaction Assurance and UK Subject matter expert on a range of other international fora.*
   - The Bill must cross-reference to the Data Use and Access Bill. It must also define what is "legitimate interest". This is needed in healthcare for which we need secure data sharing. The DUA Bill needs to be framed in such a way that it takes into account the need to share data securely.
   - Govt. departments need to talk to each other. Without this we will be in a mess.
   - The Bill must take into account the risks to loss of personal data from (presumed?) lack of security controls
   - CFIT (https://cfit.org.uk/) are looking at how fin and regtech can work together.
   - Need for joined up legislation and government

b) **David Cook, DLA Piper** - *David Cook is a Contentious Cyber Security and Data Protection partner at DLA Piper, a global law firm. His practice is focused on advising with respect to three linked areas: (1) cyber security governance and controls; (2) cyber security incident response; and (3) the various elements of scrutiny applied following a cyber security or data protection incident. His background is in coding and having a technical mind and that influences his practice: his career began advising alleged hackers and cyber criminals; he was instructed by police and government to advise on cyber crime prevention and cyber* *security governance; and corporate instructions followed. He advises the biggest organisations on their most important cyber security and data protection issues, including many of the high profile "hacking" events that are covered in the media and many more that are not(!).*

- Need to look at this in an EU and Worldwide context, this is not a time for divergence. The Kings speech referred to inherited EU Laws and that was an implied reference to the EU Network and Information Systems Directive, which was transposed into UK law by way of the NIS Regulations 2018.
- EU is overhauling NIS 2018, focus on Operators of Essential Services, less so on Relevant Digital Service Providers. Emphasis is on the importance of supply chains
- Slide 6: attacks are often on vulnerable parts of the supply chain. In the US many states impose duties on Company Directors. NIS2 looks to mirror this.
- Slide 7: GDPR refers to "appropriate measures". These change over time as does cyber security. NIS 2 goes into greater depth as it seeks to create a more holistic approach to cyber security and align with what professionals in the sector are doing.
- Slide 8: there is no advantage to divergence. Many companies operate internationally and therefore level-up to the more rigorous cyber security frameworks.
- Slide 10: Shows the EU Digital Decade strategy. Many points on the wheel lack a UK equivalent. We need to keep pace with the EU.
- Slide 12: If we move now we will not fall behind.

c) **Freha Arshad, Accenture** - *Freha leads Accenture Security's UK&I Health & Public Service Practice as well as being responsible for the cyber team in Scotland. Freha is also a member of the Scottish Government's 'National Cyber Resilience Advisory Board', advising ministers and the national cyber resilience team on the cyber landscape for Scotland and how the government should best formulate its processes and action plans for a cyber resilient Scotland. Freha works in close collaboration with key stakeholders including the regional cyber cluster, with whom she co-founded 'Women in Cyber Scotland' group.*

- While sharing a common goal of protecting critical infrastructure and supply chains, the two legislative frameworks (CSR & NIS2) could also present distinct differences.
- There is no mention of fines in the CSR Bill's announcement and there is no indication about whether they will be introduced later down the road or not. But, with the relative success of GDPR's fines, even as a scare tactic, it would be reasonable to expect some kind of punishment for non-compliance.
- Wants consolidation of legislation for companies / organisations.

- Data sharing requirements, in principle, make sense. How do you implement this in practice? Do I share IP addresses, how do I protect my commercial interests and what about anonymous reporting? Key question: how is this data is going to be collected in a privacy-conscious manner and then disseminated without revealing where the attack is taking place?
- What are the drivers for rationalisation across the framework?

Open questions and discussion

a. AC – we should see NIS2 as a direction rather than a regulation.

b. AC – Financial Services are exempt but have strong, sector-specific security requirements. The UK is leading the world on Open Banking and this gives us a head start on everyone else.

c. DC – There are other laws such as DORA from the EU which do effect the FS sector. This sector is globally ahead of the pack but we see threats changing all the time. Many of these FS companies work across borders anyway so will need to conform to local laws wherever they operate.

d. Dominic Connor – we are woefully unprepared. There are some bastions of good security but our ability to cope is, in general, not good. Audits can miss things. In particular fears that small suppliers are vulnerable to attack. The Insurance industry is not paying out.

e. Carla Baker – Bill cannot cover everything and should focus on the Critical National Infrastructure. Divergence and alignment are key.

f. Stewart Room – EU legislation is more prescriptive because, in part, it has to cover 27 countries and not just one. If there is a legal duty of care then you do have what you need. Bill should avoid going into details such as how many characters in a password. Sees two problems:

    a. The first is about the technology supply chain in its widest sense. NIS put a duty of care on the suppliers of the technology, NIS2 goes wider and covers the user community as well.

    b. Fines for Directors will have a chilling effect. Put in an FOI on HMG and received no real answers.

   Focus on the supply chain.

g. Kuan Hon – DUA and GDPR are good for personal data. NIS2 for resilience and non-personal data. We should regulate those who provide the security. Also we do not publicise the CNI list as that would tell our enemies whom to attack. However, one regulator insists on revealing the full supply chain which is part of the CNI, this is a threat to security! There are many examples of outdated practices being forced onto suppliers. The Bill should prevent this. We have the Product Security and Telecommunications Infrastructure Act 2022 which could be expanded to cover more device types. Why do we have 24 hours to report a breach and not 72, what difference does this make?

h. Steve Penny, SANS Institute - at the SANS CISO summit, the asks are for clarity; interoperability and a rationale behind the breach reporting requirements. Should there also be, through the Cyber Security Council, a licence to practice? What about training in schools?

i. Baroness Pauline Neville-Jones
   - What's needed for legislators? To be clear on the purpose of legislation and its scope / limits. What is the extent of the legislation's ambition and likely effect?
   - What lies outside the legislation, i.e., the bigger picture, other pieces of (possibly) intended legislation?
   - Wants thoughts around the content of the bill and the extent of divergency of UK legislation from the EU and USA

j. Carla Baker – Agrees that EU approach is prescriptive. UK does not need to legislate in the same way to get the same outcomes. The Bill should have more on skills. Needs also to take into account US standards. Cannot solve everything so focus on supply chain.
k. Lord Arbuthnot – absence of skills is the greatest threat.
l. Lord Hogan-Howe – would like to look at DC's circle slide in greater depth.
m. Gerard Philips – we should avoid a legal quarrel with the EU and the US.
n. KH - Adequacy arrangements need to be worked out as we will need to be able to transfer data.
o. Arthur Virgo – goal is practical security.
p. Luke Barton – focus on skills is key.

Conclusions

Lord Arbuthnot: we will need a second meeting and AH will lead the work in the meantime to put together the ideas in a coherent way.