APPG ON CYBER SECURITY AND BUSINESS RESILIENCE MEETING
3RD FEBRUARY 2025, 3.30 P.M. COMMITTEE ROOM G, HOUSE OF LORDS

Title: The purpose of the meeting is to review and expand on the work of the December meeting which looked at preparing a brief for Parliamentarians to cover the forthcoming Bill on Cyber Security and Resilience.

Chairman's welcome: Baroness Neville-Jones started the meeting and welcomed the speaker and attendees.

Present: Baroness Neville-Jones, Earl of Erroll, Lords Hogan-Howe and Sharpe, Kit Malthouse MP (APPG Chair).

Apologies: Lords Alderdice, Arbuthnot, Mackenzie of Framwellgate and Taylor of Warwick.

Speaker: **David Cook, DLA Piper** - *David Cook is a Contentious Cyber Security and Data Protection partner at DLA Piper, a global law firm.*

Our aim should be to build a business community that works in the UK and benefits the UK economy. We do need to be mindful of our relationship with the EU and the US, who are clearly key trading partners.

While there is a temptation to consider these new laws in isolation and what works best in the UK only and for UK business only, that would be a potentially fatal mistake. The simple truth is that we are not alone, our businesses are increasingly global in nature and so sit in a global legislative framework.

The EU is pushing the Digital Decade suite of laws that are designed to ultimately see the digital economy prosper across the EU but does that through setting out a comprehensive framework of new laws that this initiative sits on. We risk falling behind if we do not align with the EU. Currently we are falling further and further behind what the EU is doing.

In the King's speech, reforms of the NIS Regulations 2018 were flagged up in the guise of the forthcoming Cyber Security and Resilience Bill. It appears to be based on the EU NIS1 Directive upgrades in the form of NIS2 which is more focussed on a wider range of threats and industry players. It is also to be hoped that:

a) the Bill will remedy the lack of enforcement to encourage companies to tighten up on their cyber security policies etc. This could be a mix of directives, enforcement or fines. NIS2 brings with it a stronger enforcement regime.
b) The Bill will look more closely at how we make supply chains resilient.

This is not an official publication of the House of Commons or the House of Lords. It has not been approved by either House or its committees. All-Party Parliamentary Groups are informal groups of Members of both Houses with a common interest in particular issues. The views expressed in this report are those of the group. The APPG is sponsored by the Institute of Corporate Resilience, SANS Institute, DLA Piper, Accenture and the Information Security Group, Royal Holloway College.

If we diverge from the EU and soften our regulatory environment, will that leave us more vulnerable to cyber attacks? All businesses that operate in the EU will be following EU legislation anyway so it would lead to no meaningful change for them – they still have to do it. The difference is that the UK government won't have visibility of issues affecting the UK, because there will be no obligation to report here. Should there be a stronger regulatory and sanctions (enforcement or fines) for businesses which are not up to scratch? Business are saying that they do not want to be overregulated.

All of this is against a background of changing geopolitical threats from Russia, China, North Korea, Iran and others. We are also seeing more threats from Quantum Computing and zero day attacks and even really simply things like a lack of multi-factor authentication.

Open questions and discussion led by:

1) Steve Penny from the SANS Institute shared findings from various roundtables run by the Institute. Will share the results of two recent meetings of CISOs one is the nuclear sector working group. One point to bear in mind is professionalisation of the Cyber Security sector. Will this be touched on in the bill? and

2) Dr Claudia Natanson MBE, CEO, UK Cyber Security Council

The Security Council came into being in 2021. We are proud to be the only country which has actually decided to professionalize cyber security and have been inundated by many other countries asking us how have we managed to do that? The government has asked us to create standards to ensure integrity and ethics. We need an overarching body able to implement standards and ensure ethics and integrity in this sector. We work hand in hand with the NCSC who are the technical arm for protecting our country and of course the Department of Science, Innovation and Technology which funds the Council.

We are the only body to whom the government has elected to award Cyber Security titles which are aligned to the Councils Standards for Cyber Security Competence and Commitment for a professional.(SPCC)., You can therefore receive the award of Chartered Cyber Security Professional (ChCSP). We also award titles Cyber Security Principal (PriCSP), and Cyber Security Practitioner (PraCSP) . The Council has an Associate level (ACSP)which is not aligned to a specific specialism but is an entry level path into the cyber security profession. The Council is committed to keep diverse pathways open into cyber security.

The UK needs more specialists in testing, system design, governance and risk manager and audit and assurance. In 2025 we are releasing four more specialisms:

i) cyber security management which will help to translate the topic at Board and executive levels into English;

ii) Incident Management
iii) Operations, coaching cyber security in the physical environment.
iv) Risk Management: we know that the common denominator for everything that joins everything is data. This looks at what is the financial and organisational risk for a business?

James Staner - Do we want to end up with a jigsaw of regulations like they have in the US? Can we do divergence with a difference in the UK?

DC - We probably do not want to have a less onerous regime than the EU. Need to ask:
What do you want to do with the legislation? May need to start with a framework such as NIS2 with personal liability as this gets people attention.

Baroness Neville-Jones – we need to ensure equivalence of outcome.

Andrew Churchill - In the US a significant cyber security incident is called a material incident. SEC rules mandate reporting it within 72 hours. Financial Services have been exempt because they already have strong sector specific security standards. Not clear if the FS exemption will be transposed into new legislation. In the Data Use and Access Bill, under the regulatory impact assessment, all smart data builds on open banking. Thus we have just built all of our data onto an exempt sector. In addition under DORA, the NIS2 standards will be implemented in 27 different ways. This will effect supply chains where these cross EU borders and could cause confusion.

Keith Scott - Are we supporting principles, standards or outcomes? I think outcomes
are really important here. Standards have their place but we are trying to nudge culture here through. You always find companies to help you get through to that minimum standard.

Kostas Markantonakis – need to unleash innovation. Standards can help to shape innovation.

Iain Philips – standards need to be managed
SP – standards are easy to measure and define.

Roy Isbell – ENISA looked at the cyber security of ports. Defined seven levels of maturity. They had lots of standards but not always in the right place!
DC – not the case that bad companies fail due to a cyber attack. The Regulator needs to be more active. Compare the Health and Safety Act. A whole ecosystem built up around health and safety thanks to the Act.

Mike Hurst – what will the legislation do to prevent crime and allow for detection? Big companies need to share information to help detection. It is not easy to link crimes up across different companies as information cannot or will not be shared.

Lord Hogan-Howe – the Insurance industry is a really good at sharing data about people who double claim. There is a clear win from sharing that data. The Financial Services sector do not share data. The fact is that they are victims and they see it as a commercial risk. I would say it is a community risk. They require the individual client to declare their financial situation. I think it's a really strong point. You can share data about people without actually naming them, you can minimize the data, then you can spot patterns.
Insurance can be used to drive behaviour. Insurers have changed our behaviour through premiums, this gives us an incentive to change.

Ben Lyons – AI has come into play since NIS1 which has just expanded the attack surface. The Bill must take this into account. Would like to see continuous monitoring and speed of response / recovery included in the Bill. Furthermore protecting supply chains is going to be very important. The UK does not seem to be going as far as the EU with this We also need to think about how to protect data centres.

Dr. Ashima Chopra – two points

1. The threats are growing and AI is exacerbating them.
2. An impact-based approach will encourage innovation, need to go beyond just outcomes.

Roy Isbell - Thinks software and Hardware suppliers should be held liable. They need to test their products before they launch them.
DC – need to look at a cost recovery mechanism and mandatory reporting of breaches. We also need to consider the extra-territorial nature of the Cloud whose services are often place agnostic. Who will compel a vendor to act if they are outside the UK?

Iain Philips – As consumers we have no idea where our data is nor who is manipulating it.

Lord Hogan-Howe – outsourcing one's data to Cloud should include knowing where that data is. How does an employer control data when staff move it into their own personal email or onto their own system because they have better software at home
DC - The majority of computer science courses do not include any meaningful, security education, whatever. The NCSC is accrediting degrees as well.

Robin Weir - Hong Kong lawyer. China requires clearance to export data overseas to any jurisdiction. This comes from the cyberspace administration of China which is the regulator. In view of what was said about extra territoriality and data leakage should this be considered?

Kostas Markantonakis – where does liability lie? We need to encourage both data sharing and a system that produces an insurable loss. The Insurance industry has a huge role to play in this.

1. we can learn from other sectors and environments e.g. GDPR is a great success as it puts the citizen at the centre of decision making. Is there something similar that can be done for cyber security?
2. Reporting something and being able to respond to it are different matters. You can have the mechanisms to report an attack but not the tools to respond?

At Royal Holloway we operate at under/ postgraduate degree level. It takes a generation for things to change. Thus at what level should we pitch the discussion about cyber security? All this discussion about education and training should be aimed at enhancing performance.

Conclusions: Kit Malthouse MP
Can the secretariat draft the body of a letter for the Minister with three points that should be considered in the Bill so that we can tease out where the thinking actually is?

Non-Parliamentarians present:
Andrew Henderson - Secretariat
David Cook – DLA Piper
Prof Kostas Markantonakis, Royal Holloway
Prof Roy Isbell
Prof Keith Scott, De Montfort University
Robin Weir
Iain Philips, Loughborough University
Dr. Ashima Chopra, Datambit
Ben Lyons, Darktrace
Steve Penny, SANS Institute
Freha Arshad, Accenture
James Morris, The CSBR
Andrew Churchill, The CSBR
Joe Lomako, TUVSud
John Moorcraft, TUVSud
Mike Hurst
Kris Blamires
Dan Howl, BCS
Joel Gladwin, Intuit
Dominic Connor
Simon Staffell, Microsoft
Dr Claudia Natanson MBE
James Staner, CompTIA