Event write-up: Raising cyber security standards for government suppliers

Speakers

Andrew Miller, Partner - Cyber Security Government & Health Industries, PwC

Emma Green, Head of the Cyber Security Incentives and Regulation Team, Department for Digital, Culture, Media and Sport

Peter Yapp, Deputy Director, National Cyber Security Centre
George Brasher, Managing Director UK&I, HP

Robin King, Strategic Advisor, Cyber Prism Group

The BSA, in partnership with HP, held an event on the key cyber security challenges facing the UK, and how the public sector can ensure - and enhance - high standards of cyber security within its supply chain.

Recent cyber incidents, both in the UK and globally, have shown that government departments and their suppliers remain vulnerable to attacks. In 2018, the Cabinet Office issued a new minimum set of cyber security standards that government expects departments to adhere to and exceed wherever possible. At a speech in June last year, Cabinet Office Minister David Lidington MP stated that this new standard will also apply to government strategic suppliers.

Andrew Miller from PwC began by introducing the panellists and some of the key themes for the day. He also discussed the findings of recent research done by PwC in conjunction with the National Cyber Security Centre (NCSC) and industry to uncover 'Operation Cloud Hopper', thought to be one of the largest ever sustained global cyber espionage campaigns. By targeting outsourced service providers, a group was able to access the intellectual property and sensitive data of those companies and their clients globally. The campaign highlighted how important it is for government and its suppliers to have a comprehensive view of the cyber threats their supply chain face.

Emma Green, Head of the Cyber Security Incentives and Regulation Team, Department for Digital, Culture, Media and Sport (DCMS), then provided an overview of the UK government's approach and the importance of cyber security in building the digital economy. Cyber security threats are evolving rapidly and there was an urgent need for government and businesses to improve their cyber risk management. In support of this government has implemented a minimum cyber security standard across departments with the intention of extending to its supply chain; alongside this, the accreditation scheme Cyber Essentials and guidance produced by the NCSC such as the '10 Steps to Cyber Security' and forthcoming 'Board Toolkit' provide advice and guidance to industry on assurance of cyber risk management across organisations. DCMS have also led the government work on improving cyber skills, both within industry and wider society. In December the department published the results of independent external research which explores the UK cyber skills labour market and cyber security skills gap, and the department has also issued a call for views on its initial Cyber Skills Strategy (closing on 6th March) with the intention of publishing a final strategy later this year.

The next speaker was Peter Yapp from the NCSC, who discussed the agency's ambition to make the UK the safest place to live and work online. The line between criminal and state actors was increasingly blurring, making it difficult to distinguish between the two, and an open dialogue between public and private sectors was therefore necessary to identify issues in a transparent way. He highlighted the Industry 100 initiative, which promotes close collaborative working between the NCSC and industry personnel, and the joint industry and government Cyber Security Information Sharing Partnership (CiSP) set up to exchange cyber threat information securely and in real time. However, he recognised the need to work with every sector, noting the attacks on service providers in Operation Cloud Hopper. More often than not, systems are compromised as a result of basic mistakes rather than highly sophisticated attacks, Peter said.

The session then turned to industry, and how businesses are responding to this changing landscape. George Brasher, UK&I MD for HP, highlighted how the company's approach to cyber security had changed over time. First, there had

been a change in strategy from simple defence and protection towards resilience and recovery – bad actors will always have the potential to be a 'step ahead' so businesses need to be ready to respond in kind. Second, cyber security needed to a core part of a business's products and services – 'built-in, not bolted-on', in George's words. As such HP has become one of the first industry partners to sign up to DCMS' new Internet of Things (IoT) security code of practice. Lastly, George raised the importance of public tenders and procurement as a tool for embedding effective cyber security standards to mitigate security risks within devices such as printers and laptops which are often seen as easy targets for hackers.

The final speaker was Robin King from the consultancy Cyber Prism Group, who provided an SME perspective. Robin remarked that the importance and understanding of cyber security had shifted significantly through his career, with the risk it posed moving beyond the defence agenda and into wider society. Large businesses with SMEs in their supply chain need to work more closely with them to deal with cyber threats, and move towards seeing them more as 'capital' – for the specialist skills and value they can add – than 'commodity'. The government also has a target spend of 33% on SMEs and while good progress has been made, this remains a long way from being achieved due to the complexities of tendering. Robin concluded by saying there might be a better approach to the whole issue by reconceptualising cyber security for the value it can provide, in terms of enhancing skills and the use of data, rather than by viewing and measuring it against the risk of loss.

In the wide-ranging audience Q&A that followed, one of the topics raised was whether government would bring in a 'rating scheme' for businesses and suppliers to check their cyber assurance. Panellists said there may be merit in such an approach and it would be worth piloting with companies, but there were some limitations and that approaches such as the use of narrative reports could also fulfil a useful function in demonstrating industry adherence to high standards. Another issue raised by industry was how cyber security practices could be embedded within contracts so they do not add to the cost of doing business or the complexity of bidding for contracts. Many sectors, such as construction and FM services, are operating on low margins and already face a high number of compliance checks. The panellists noted the challenges around this and said it was imperative for suppliers and government to work together to get a consensus and embed the minimum standards in the absence of stronger legislative compliance.

The role of government procurement in driving standards was also discussed more broadly. This had two elements: both the technical question of how best to use this as a tool to raise standards, particularly given the challenge of having a uniform approach across different departments, and the need for building the commercial skills within the civil service to be able to ensure robust supply chain management. Answering these questions would also have implications for the number of SMEs who take on public contracts, as expanding the base of suppliers would inevitably require a greater number of professionals to manage multiple contracts. Organisations such as HP can operate at scale and provide standardisation. Other issues raised included the challenges for charities and social enterprises, who often lack the resources and capability of other large government suppliers to manage risks, the UK's Cyber Security Clusters, and the need to drive cultural change across the public and private sector to take cyber hygiene seriously at all levels of an organisation.

Further reading

- **NCSC, Cyber Essentials:** https://www.cyberessentials.ncsc.gov.uk/
- **NCSC, 10 steps to cyber security:** https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security
- **NCSC, Cyber Security Information Sharing Partnership (CiSP):** https://www.ncsc.gov.uk/section/keep-up-to-date/cisp
- **NCSC, Industry 100:** https://www.ncsc.gov.uk/information/industry-100
- **DCMS, Cyber Security Skills Strategy:** https://www.gov.uk/government/publications/cyber-security-skills-strategy
- **PwC, Operation Cloud Hopper:** https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html
- **HP, 'The Wolf' cyber security film:** https://www8.hp.com/us/en/solutions/security/thewolf.html
- **Cyber Prism:** https://www.cyberprism.net/index.html