Public Chairs' Forum and Association of Chief Executives seminar

Cyber security: are you managing the risks?

Event Summary

PCF and ACE were delighted to host an event on 11 September 2017 on Cyber Security. In light of the ever increasing risks of cyber-attacks, the aim of this workshop was for members to hear the perspective from an arm's-length body (ALB); data privacy and the international threat of cyber-attacks; and the latest thinking from central government and the National Cyber Security Centre (NCSC). Members also had time for Q&A and group discussion.

Claire Bassett, Electoral Commission

Claire Basset, CEO of the Electoral Commission (EC), began the seminar by talking about her experiences running an ALB that operates across a large digital platform. Within the past year alone the commission has been involved with the collation of votes for the EU referendum and a snap general election – both high-profile events involving a range of different threats. TV debates, vigorous campaigning and cross-party alliances played a big role in stimulating nation-wide interest. The timing of the General Election announcement was also significant, as it was shortly after the WannaCry ransom malware attack, the terrorist attack in Manchester and the leak of candidate's information during the US election.

The referendum brought an added challenge to the EC in that certain responsibilities are devolved to local authorities, yet the Commission was required to collate the overall result of the votes. With expert advice, the Commission built the collation system in-house. Claire felt it was important for organisations to understand when they need to work with partners to build the strongest systems and mitigate risks.

Claire also noted that human risk will always be an issue that leaders must be aware of and therefore know how to work reactively as well as proactively. She used the example of ineligible voters being sent polling cards in error. Claire was keen to emphasise the importance of responding swiftly on social media to set out the facts – in this case that they still could not vote if they were not on the electoral register - as people's perceptions are as important as cyber risk. The EC has been subject to numerous conspiracy theories about altering votes; however, their strong communications team is able to deal with these effectively by being able to respond on social media without laborious sign-off processes.

Preparedness and confidence are also key: the EC ran rigorous staff training programmes and worked with all local authorities to run a test referendum count. Claire criticised the move by some local authorities banning staff from opening all attachments, which was disruptive to working effectively. She felt that it better for efforts to be made in training and engaging, with a combination of proactive and reactive measures to reduce risks. On the night of the Referendum, the EC still suffered an unsuccessful Distributed Denial of Service attack. However, they responded quickly and worked with the NCSC to produce joint guidance for local authorities on how to respond when attacked.

Professor Eerke Boiten, Cyber Technology Institute

Professor of Cyber Security Eerke Boiten from De Montfort University's Cyber Technology Institute talked about the risks surrounding attacks on personal data in public sector organisations. He was keen to emphasise the importance of sharing cyber intelligence and having a co-ordinated response from the centre. Boiten also noted that ALBs should be weary of the fact that data privacy can often be an international issue and organisations may be working beyond the scope of national government regulations, such as the General Data Protection Regulations (GDPR). Therefore, the fines and regulations GDPR puts on organisations in the UK may not have the same impact and is important to rely on such regulations. Again, he reiterated that managing reputations, staff training and preparedness are imperative.

Emma Green, DCMS

Emma Green, Head of Digital Economy, Society and Engagement at DCMS spoke of the manifesto commitment of a digital charter to make the UK the safest online, had led to DCMS's remit to make all ALBs aware of cyber security issues. Shockingly, she reported that between 66-68% of enterprises have experienced a cyber security breach within the past year and while many organisations have firewalls in place and restrict IT access to certain users, only 20% of staff have received cyber security training. Within ALBs, she stressed the imperative of cyber security being an issue for the whole board, not just the IT department. Following the '10 Steps to Cyber Security' (shared in the accompanying powerpoint) ALBs must ensure their attempts to safeguard their organisations include all aspects of risk, including: network security, user education, malware prevention, media controls, secure configuration, managing user profiles, incident management, monitoring and developing safe mobile working policies.

Cyber Essentials is a government-backed cybersecurity certification scheme developed by the NCSC, which sets out a good baseline of cyber security suitable for all organisations in all sectors. DCMS is working hard to implement its standards across government and ALBs.
https://www.cyberaware.gov.uk/cyberessentials/

DCMS is also driving the GDPR and working closely with the Information Commissioner's Office to ensure they appropriately regulate government cyber protection. Emma also mentioned that DCMS is working with the Department for Education to incorporate cyber security into the national curriculum to ensure people from a young age understand the risks involved when working on a digital platform.

National Cyber Security Centre

Alison Whitney, Deputy Director for Digital Government at NCSC gave members an overview of their role and opportunities for ALBs.

NCSC is still only a year old but is here to make the UK the safest place to live and do business online. NCSC has four key aims:

- Reduce the cyber security risk to the UK;
- Respond effectively to cyber security incidents – as it is not possible to be successful 100% of the time, it is important that organisations know how to respond. ALBs are responsible for their own risks, but NCSC's role is to help mitigate those risks and help public bodies respond accordingly.
- Understand the UK's cyber security environment, sharing knowledge, addressing systemic vulnerabilities; and
- Nurture the UK's cyber security capability, providing leadership on key national cyber security issues.

The types of threat actors (criminals, hackers, state actors, terrorists, insiders) and their motivations are very important for organisations to consider. There is guidance on the NCSC website on these areas. The NCSC work with ALBs but where they bring the knowledge of attackers, threats, strategies for defence, they also need organisations to know their business and what it is that they do that would interest attackers. For example, does the ALB hold a large amount of citizens' data, staff data, handle large sums of money, or is there risk of organisational and personal reputational damage?

The NCSC provide many services, such as the Active Cyber Defence (ACD) programme. ACE members were presented with information on four extremely successful aspects of ACD:

- Takedowns – the NCSC offers a takedown service which protects government brands from phishing and malware.
- DMARC – this is a technical, international standard, which, if implemented, verifies the legitimacy of your domain. There is guidance on the NCSC website on how to implement this. DMARC also means that when someone tries to impersonate your brand, they are automatically blocked, and the ALB will also receive a copy of their attempt, as the owner of the domain.
- Protective DNS – NCSC is working with GDS to provide this service to the public sector free-of-charge. Certain sites that NCSC know are risky or carry dangerous malware will return a block page when clicked on. 44 organisations are currently signed up with large-scale success.
- Web Check – organisations know they are supposed to keep systems up-to-date and that technical testing is good, but often lack the expertise to carry them out. Web Check was developed in partnership with local authorities and others and enables users to check that their websites are free from common vulnerabilities, providing plain English guidance on how to deal with any problems

that are identified. Organisations can sign up for the service via the following link: https://www.webcheck.service.ncsc.gov.uk/

Members were invited to read the weekly threat report on the NCSC website at https://www.ncsc.gov.uk/index/report and join the Cyber Security Information Sharing Partnership (CISP) https://www.ncsc.gov.uk/cisp. NCSC' annual report is also available https://www.ncsc.gov.uk/news/2017-annual-review

NCSC asked attendees to discuss the following questions in groups;

- How does your organisation currently approach cyber security?
- What challenges and opportunities does your organisation experience when adopting good cyber security practices?
- What more can we do together to overcome the challenges and exploit the opportunities?

Some of the key themes to emerge were:

- **Governance** It is important for cyber security to be seen to be an issue discussed at board level to breed importance through the organisation. Members agreed having a lead board member for cyber security was a good idea, however sometimes board members are apprehensive to take on the responsibility. The NCSC agreed that all enterprises have vulnerabilities, not all risks can be eliminated or foreseen, and that if their advice was followed and attacks still arose they would support organisations during any subsequent enquiries. In the event of a major incident. They also reiterated that cyber leads do not necessarily need to be technical experts (that is what NCSC is there for!), just bring their in-depth understanding of the business to the partnership.
- **Sharing best practice** Many Chairs and CEOs are new to cyber risk. They welcomed opportunities to share lessons learnt. While NCSC's 'CISP' is an information sharing platform this is often at quite a technical level and NCSC said that they would consider ways to facilitate board level information sharing. They invited members to send in case-studies and experiences that they can anonymise and put on the website.
- **Guidance** Members would welcome benchmarking for best practice and what services provide value for money. Some members reported that they have received guidance from NCSC that conflicts with other government sources and welcomed clarity. Alison noted that NCSC's risk management principles and cyber essentials (available on their website) offer a good understanding of what good cyber security looks like. Cabinet Office is also producing principles in line with NCSC's work. It was noted however that guidance must not be a tick-box exercise and that risk must be considered in relation to the ALB's systems and business.
- **Usability of systems** It was agreed that there should be a balance between security, and the efficiency and usability of systems in the workplace. For example, the health sector being able to access relevant files quickly when needed without laborious security procedures.

Unfortunately NCSC did not have time to answer all the questions from the table groups. However, it has since responded with the following;

- How do organisations mitigate a sense of optionality and keep continuously focused on cyber security issues?

The NCSC recommends that boards ensure that cyber security is included on their corporate risk register and reviewed regularly at senior level. As discussed at the event, effective governance is essential and boards should ensure that it is clear throughout an organisation that the senior responsible and accountable officers are for cyber security. All staff should be provided with basic training to enable them to recognise cyber security risks in their business and provided with regular refreshers.

- Should organisations use the cloud? What are the risks?

Cyber security risk management is contextual: an organisation needs to be clear about the business outcomes it is trying to achieve and the technology options available to it. Cloud-based solutions may be suitable and appropriate to meet some of these. The NCSC itself uses cloud-based solutions to meet some business needs. There is guidance on cloud security on the NCSC website: https://www.ncsc.gov.uk/index/guidance?f%5B0%5D=field_topics%253Aname%3ACloud%20security

Some members felt that before this presentation they knew very little about NCSC and the services that are available to them. They welcomed more contact from NCSC or central guidance on these services to send thorough their organisations.