What we learned from...

SASIG Thought Leadership Summit

A Critical Appreciation of Cybersecurity Resources Supporting UK Media and Broadcasting Sectors

About this whitepaper

SASIG held our Thought Leadership Summit on Wednesday 21 June in collaboration with the UK Cyber Security Council. Our objective was to provide an in-depth look at the cybersecurity resources supporting the UK media and broadcasting sectors. A wide cross-section of speakers representing public and private sectors, including the government, contributed to the event.

The objective of our seminar was to inform delegates who amongst the government agencies has responsibility for cybersecurity and resilience and what their respective remits are, how they align and synchronise with each other, and how their services and resources can be accessed and used by enterprises of all sizes and sectors, both public and private.

Executive Summary

SASIG's Thought Leadership Summit on 21 June, in collaboration with the UKCSC, focused on an appreciation of cybersecurity resources supporting the UK Media and Broadcasting Sectors. NCSC, DSIT, NPCC, NCA and NPSA contributed to the presentations, as well as the UKCSC and the NCAB. This provided an overview of the capabilities within government able to support the sectors including their roles and responsibilities.

NCSC, as the National Technical Authority, provides advice and, where appropriate, intelligence to UK-based enterprises to inform and improve resilience. As the public-facing arm of GCHQ, it offers a unique perspective, as it is neither a policy-making department nor a regulator. This enables it to provide advice without prejudice. DSIT remains the pre-eminent government department to generate policy on cybersecurity, including legislation, as well as capabilities available to assist organisations to improve their resilience posture. DSIT and NCSC presented jointly, demonstrating their close collaboration.

Combating cybercrime falls directly to UK law enforcement (LEA) as the executive arm of government. The NCA's National Cyber Crime Unit explained its role in combating cybercrimes such as ransomware and its specific responsibility to disrupt criminal networks operating across multiple jurisdictions. Collaboration with overseas LEAs remains key to achieving this. NPSA, which has replaced CPNI, has a new remit to extend its outreach beyond CNI and will play a role in helping enterprises to improve resilience, along with the established role of the NPCC through its regional CRC and other initiatives.

The UKCSC continues to strive to define and improve the professional standards of the cybersecurity sector. To achieve this, it encourages dialogue with consumers whose needs should be paramount. The NBAC continues to support the UKCSC in this.

A panel discussion with CISOs from the sectors emphasised the need for intelligence sharing and close collaboration between the public and private sectors. The panel demanded action rather than words; not just an aspiration to improve how we collaborate but concrete steps to make this happen. This theme was also echoed by the keynote speech from the MoD which underlined the importance of defence, no matter how appealing in a military context offensive capability can be. We face common challenges which require a common approach and deeper collaboration across sectors.

An overview of the work of the National Cyber Security Centre (NCSC) and the cybersecurity services provided by the UK Government Department for Science, Innovation and Technology (DSIT)

NCSC briefed on its roles and functions, and DSIT outlined the cybersecurity services it provides. As the national technical authority (so neither a regulator nor a policy-generating department), NCSC holds a unique position in the cybersecurity landscape to provide unprejudiced advice to organisations.

NCSC as part of GCHQ, has a particular advantage in understanding and addressing cybersecurity threats. Its remit is to support government, the public and the private sector, by sharing knowledge, information and intelligence with organisations and sectors; responding to significant cybersecurity incidents; reducing cyber risk to the UK; and developing the nation's security capability. It aims to build resilience and improve cybersecurity across sectors by working with government departments, industry players, regulators, and critical national infrastructure.

We discussed how the NCSC engages and best serves the various industry sectors to ensure transparency and information sharing across multiple groups. Mapping critical elements within sectors helps NCSC to improve resilience, provide technical guidance, support, testing and threat intelligence, and helps organisations understand evolving threats.

DSIT presented its UK cyber strategy, which focuses on building UK capability and addressing cyber resilience domestically and globally. Various government departments and agencies collaborate closely with DSIT, notably the Cabinet Office on government digital security and the Department of Business and Trade to promote UK cyber products overseas. Some examples of specific interventions from DSIT include legislation covering consumer intelligent devices and a voluntary code of practice for app store providers.

DSIT described how it develops and applies different interventions, such as enhancing resilience at scale and reducing the burden upon organisations. Its recent initiatives include building the nation's cyber skills and changing market operations through accountability and regulation.

The work of the National Crime Agency (NCA) and The National Cyber Crime Unit (NCCU)

NCA has a nationwide remit, with its workforce divided into core areas such as intelligence, investigations, and technical support, each focused-on threats to the nation from criminal organisations. The approach to cybercrime is built around a framework of Pursue, Prevent, Protect, and Prepare.

NCA categorises the cybercriminal ecosystem into three principal parts: products (such as malware, ransomware, and exploit kits), goods (the sale of data and technical vulnerabilities), and services (including ransomware-as-a-service and counter services), target ing what it calls the 'five pillars' of the marketplace ecosystem: infrastructure, financial services, initial access services, marketplaces and forums, and victim support.

NCA strategically targets cybercrime marketplace enablers to prevent low-level cybercriminals from evolving into traditional ransomware groups. It disrupts cybercriminals through sanctions, in collaboration with law enforcement overseas and other international bodies, as well as executing disruption operations such as creating fake DDoS hire services to gather data on individuals involved in cybercrime.

The National Police Chiefs' Council (NPCC) and the National Cyber Resilience Centre Group (NCRCG)

The NPCC presented the cyber program they are running on behalf of the UK police forces, which is focused on tackling cybercrime and assisting businesses, especially SMEs. The NPCC speaker addressed the importance of basic cybersecurity hygiene such as patching software, using strong passwords, and implementing multifactor authentication to mitigate cyber threats. Collective defence and collaboration between the public and private sectors is also essential in combating cyber threats. For example, the Cyber Alarm system enables organisations to detect and report suspicious cyber activity to the NPCC.

The NCRCG is an NPCC initiative. Its regional centres are resources for organisations seeking support and guidance in improving their cyber resilience. Upcoming improvements to Action Fraud and the national fraud and cybercrime reporting centre were also discussed. The network of Cyber Resilience Centres continues to engage with regional communities, especially businesses to provide advice to raise awareness as well as specific capabilities to improve resilience. The NPCC has also developed specific capabilities, such as Cyber Alarm to improve awareness and resilience.

Case study – Innovating to solve big problems

Our case study focused on the importance of the human aspect of cybersecurity and the challenges associated with this. Understanding how cybersecurity is evolving and recognising how organisations can better support individuals in improving their security behaviours is crucial. The UK's research community and academic institutions are rich with knowledge and provide valuable insights into and support for cybersecurity. Significant studies into cybersecurity are currently being conducted, encouraging and helping organisations to reduce their risk.

We examined a security behaviour database that catalogues behaviours and how each correlates with a risk outcome. This provides organisations with meaningful insights to benchmark and adopt intervention strategies. This is just one way that technology can assist in behavioural change, with this all becoming ever-more automated in the future. Greater sharing of information and knowledge freely within the community will be essential if we are to manage the risks of human behaviour effectively in the future.

Security governance

The National Protective Security Authority (NPSA, previously Centre for Protection of National Infrastructure - CPNI) presented its expanded role. CPNI offered advice and resources to assist businesses which are part of the nation's critical national infrastructure to enhance their security practices and improve resilience. NPSA has an expanded remit to engage beyond critical national infrastructure and assist all companies across the UK and non-security practitioners, in order to promote resilience within businesses.

Organised crime, industrial espionage, 'hacktivism' and cyber-attacks can cause considerable damage to a business's reputation and finances, with potential legal consequences, and good governance and security practices within organisations are essential in preventing such incidents. However, there is often a disconnect between top-level executives responsible for setting policies and budgets and those accountable for daily security operations. NPSA's programme for non-security practising executives aims to help them understand cyber resilience and how what they often perceive as best practice may, in fact, be creating organisational vulnerabilities.

The role of the National Cyber Advisory Board (NCAB) and the UK Cyber Security Council (UKCSC)

The NCAB is an executive-level board of senior leaders that advises the government on cybersecurity matters. Leaders are from an array of sectors, industries, universities, charities, and SMEs. It aims to promote a whole-of-society approach to cybersecurity and support implementing the national cyber strategy. Its three priority areas are skills and diversity, digital supply chains, and risk and crisis management.

The UK Cyber Security Council is specifically responsible for setting professional standards and developing ethical guidelines for the cybersecurity profession. The UKCSC presentation explained how they assess professionals for technical competence and soft skills at three levels, for tiered membership of Chartership, Principal and Associate. The council actively engages with organisations and aims to align qualifications and certifications with the professional titles it offers through collaboration and partnerships within the cybersecurity ecosystem. It is reviewing the current set of specialisations to gauge whether they remain fit for purpose and provide the consumer community with the skills and capabilities they need.

Panel discussion – The CISO's needs, concerns and contributions

We finished with a panel session of CISOs from the media and broadcasting sector to explore whether government organisations and specialised cyber services met their needs and concerns. The panel concluded there remains a need for real-time threat information and actionable intelligence to inform decision-makers as well as proactive support and tangible feedback from government departments when dealing with cyber threats. The majority of the panellists commented that it is still not always clear which departments CISOs should engage with following an incident.

The panel recommended that government organisations should actively engage with the community on actionable intelligence and CISOs want to be better consulted in advance on regulations that affect them. Businesses should also proactively collaborate to achieve these goals.

The panel noted that organisations struggle with information overload on cybersecurity offerings which makes it difficult for them to appreciate the appropriate capability for their needs. They recommended that government provide a more rigorous framework of standards to alleviate this challenge. The panel also emphasised the need for greater awareness, collaboration, and skills development across organisations, including the board. To achieve this, they recommended that the government set clear expectations of what it expects from business, as well as enhancing the collaboration and engagement with industry players. This should focus on improving the sharing of threat intelligence, timely feedback, and improved frameworks, standards, and guidance to navigate the complex cybersecurity landscape.

Throughout the discussion, the panel acknowledged the progress that had been made in increasing resources, clarifying compliance guidance, and improving real-time information sharing. However, they also recognised the need to continue to bridge the gap between industry and government, fostering effective collaboration to address cybersecurity challenges.

Closing keynote: A case study on the Defence Cyber Protection Partnership

Our final keynote was by the CISO from the MOD emphasised the importance of collaboration between government and industry in addressing cybersecurity challenges. The Ministry of Defence's role in developing military capabilities, executing military operations and protecting the UK is important, but so is its investment in defensive cyber. The National Cyber Force continues to enhance its offensive capabilities but would be negated without a robust cyber defence strategy. The Ministry of Defence's IT environment is complex, and collaboration with industry will continue to be central to assuring it.

Innovation, research, and cooperation with international partners will remain critical in developing the UK's capability. Emerging technologies will be embraced which will require a cultural shift w a greater focus on secure-by-design to meet the evolving cybersecurity challenges.

Register for our upcoming events at thesasig.com/events

With thanks to our Supporters