Cyber Security Governance and Strategy

techUK

Evolution of the Cyber Threat

- An **increase in pace and number** of cyber security incidents
- **No increase in severity**
- Vulnerabilities are **old and can be patched**
- Attacks **do not require use of high-end skills**
- **Supply chain at risk,** with suppliers being the first source of the compromise

Cyber Resilience in the Boardroom

Cyber security is rising up the agenda at the board level.

- 74% of UK businesses rank cyber security as a priority, and large UK organisations rank among the most cyber-ready internationally.
- 77% of businesses saying that board discussion and management of cyber security has increased since the introduction.

However, challenges remain in turning cyber awareness into action.

- Less than 30% of businesses have a formal cyber policy and only 12% have set cyber security standards for their suppliers. Nearly two in five firms have no plans to take up cyber insurance.

Improving cyber resilience is a shared priority for government

National Cyber Security Strategy – 2016-2021

The current Cyber Security Strategy 2016 to 2021 sets out government's plan to make Britain more cyber-resilient and secure, supported by a £1.9 billion investment. The strategy is built on 3 core pillars:

- Defend: 'We have the means to defend the UK against evolving cyber threats… Citizens, businesses and the public sector have the knowledge and ability to defend themselves.'

- Deter: 'We detect, understand, investigate and disrupt hostile action… We have the means to take offensive action in cyberspace, should we choose to do so.'

- Develop: 'We have an innovative, growing cyber security industry, underpinned by world-leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors.'

The Role for Business

Government initially expected to look to the market to drive the behaviours that would lead to the UK becoming more cyber resilient. However, the current National Cyber Security Strategy finds that 'the combination of market forces and government encouragement has not been sufficient in itself to secure our long-term interests at the pace required.' It therefore sets out government's expanded role in four areas:

- Levers and incentives to drive up standards and incentivise innovation
- Expanded intelligence using capacity only government has to defend the UK from the most sophisticated threats.
- Development and deployment of technology in partnership with industry.
- National Cyber Security Centre (NCSC) to deliver tailored advice to business, regulators, and departments.

The Regulatory Landscape

Cyber security is firmly into the regulatory spotlight at both a national and a European level. The last few years have seen two major pieces of cyber legislation aimed at improving cyber risk management for both the broad business community and Critical National Infrastructure (CNI)

- The General Data Protection Regulation (GDPR):The biggest change to data laws in 20 years, with new requirements for incident reporting, data security and board level governance.

- Network and Information System (NIS) Directive: Updated security principles for essential economic services (e.g. energy, transport, water, healthcare, etc.). The NIS Directive is an important step in setting harmonised standards and reporting mechanisms for critical national infrastructure.

- EU Cybersecurity Act: Reinforces the mandate of ENISA and creates a framework for European Cybersecurity Certificates for products, processes, and services.

What can you do to protect yourself

- NCSC Guidance (website, board toolkit)
- CiSP
- Incident Response Plan
- Training
- Engage with regulators