Department for
Digital, Culture,
Media & Sport

LMF Cyber Resilience Summit

10 March 2022

Stuart Peters
Head of Cyber Resilience Team
stuart.peters@dcms.gov.uk

DCMS and Cyber Security

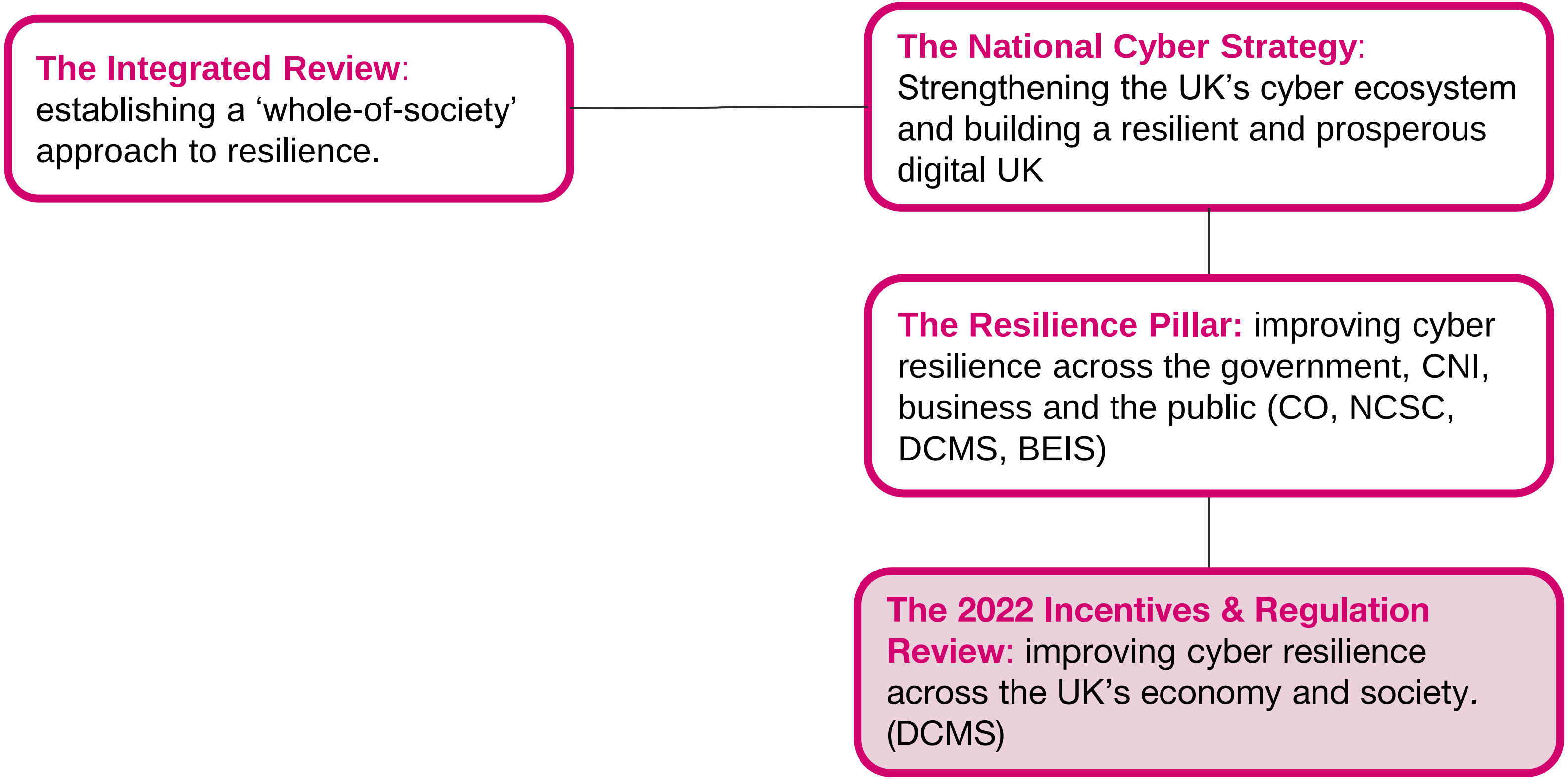
DCMS's work on cyber security is focused on:

- building and developing the UK's cyber economy;
- **supporting businesses to be more cyber resilient;** and
- looking at future technologies to see where the UK can use them to become more secure or make them more secure.

Within this, the role of the Cyber Resilience team is:

- To create the right environment to support and encourage UK businesses and organisations to become more cyber resilient.

Cyber Resilience: The Strategic context



The Integrated Review: establishing a ‘whole-of-society’ approach to resilience.

The National Cyber Strategy: Strengthening the UK’s cyber ecosystem and building a resilient and prosperous digital UK

The Resilience Pillar: improving cyber resilience across the government, CNI, business and the public (CO, NCSC, DCMS, BEIS)

The 2022 Incentives & Regulation Review: improving cyber resilience across the UK’s economy and society. (DCMS)

DCMS Cyber Resilience Policy Priorities

FOUNDATIONS	Cyber Essentials Cyber Aware Campaign
MARKET INCENTIVES	Cyber Insurance Supply Chains
ACCOUNTABILITY	Corporate reporting Governance Standards GDPR
REGULATION	Proposal for legislation to improve the UK’s cyber resilience **Consultation open until 10 April 2022**
EVIDENCE BASE	Cyber Breaches Survey, Longitudinal Survey, Captains of Industry Report,Supply Chain Call for Views, 2019 Call for Evidence, Incentives & Regulations, EAG

DCMS - Interest in the Insurance Sector

DCMS interests in the insurance sector are twofold.

First, we want you to be more cyber resilient yourselves. To make sure that you are investing in cyber security and are resilient to the threats.

Second, we want the insurance sector to promote better cyber security amongst your clients. We want the sector to amplify messages on the need for cyber security and to create incentives for companies to invest in cyber security.

- Subsequent to this last ask, we want you to encourage clients to take on Cyber Essentials, as the UK government’s basic cyber security assurance scheme.

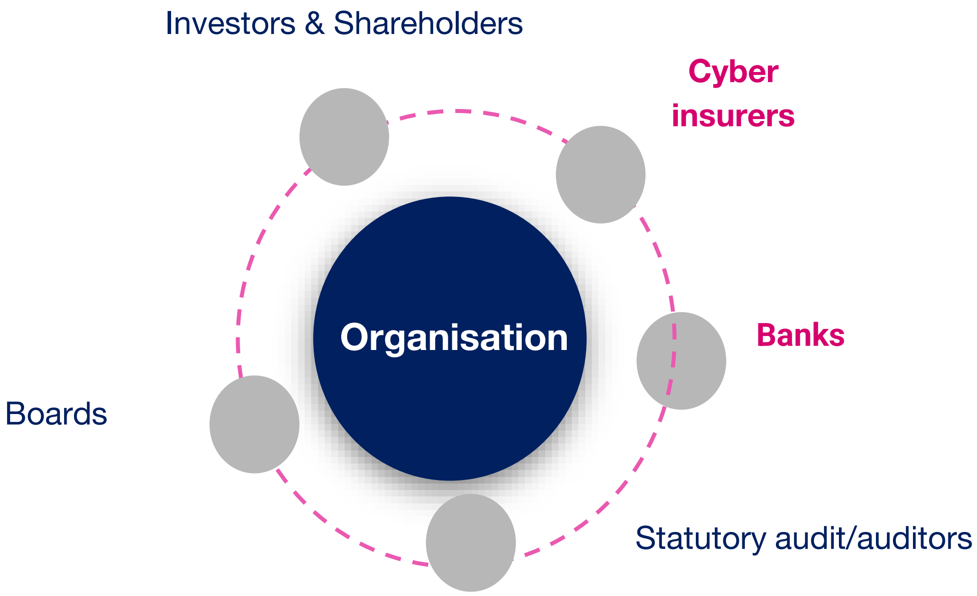
Market Incentives

The market incentives team engages with key stakeholder groups across the economy who hold market power and influence in the cyber security landscape, i.e. ‘market risk managers’.

1. The 2019-20 Call for Evidence (CfE) showed that **71% of respondents agreed that a lack of strong commercial rationale** was a barrier for effective cyber risk management.

1. The CfE found that there are a number of **information failures** preventing organisations from conducting robust cyber risk assessments, including on the threat (frequency and severity), impact or harm of cyber incidents, and mitigation activities and associated costs.

1. Organisations therefore find it **difficult to demonstrate a return on investment in cyber security** as they are unable to quantify the level of cyber risk, and **therefore cannot justify investment in cyber risk mitigations**.



What role does the insurance market play in improving cyber resilience?

- The 2019-20 Call for Evidence (CfE) showed that **71% of respondents agreed that a lack of strong commercial rationale** was a barrier for effective cyber risk management.
- The **2022 National Cyber Strategy** outlined Government’s interest in working with insurers to **incentivise good cyber security practices across the economy.**
- Cyber insurance not only offers a risk transfer mechanism, but also offers pre and post-incident services to insureds. Pre-incident services, e.g. active cyber defence, can help defend against cyber attacks and post-incident services can help organisations recover faster.
- Government will be engaging with the cyber insurance industry, through a trust group led by the NCSC. Through this group, industry will be able to understand the threat landscape, influence government decisions, and NCSC will share key advisories and threat information as and when incidents happen, so being part of the group will ensure you are the first to receive relevant releases of information. In return, Government hopes to gain access to data relating to ransomware, impact information and upcoming threats.

What is Cyber Essentials?

- The Cyber Essentials (CE) certification scheme helps organisations, regardless of size, improve their cyber resilience and **protect themselves against the most common internet-based threats/attacks** by supporting them to achieve **5 basic technical controls**:
    - **Firewalls & Routers:** Use a firewall to secure your internet connection
    - **Secure Configuration:** Choose the most secure settings for your devices and software (i.e. passwords, 2FA)
    - **Access Control:** control who has access to your data and services
    - **Malware Protection:** Protect yourself from viruses and other malware
    - **Software Updates:** Keep your devices and software up to date

- CE represents **bare minimum cyber security standards**.

What impact is Cyber Essentials having on building resilience?

- As of the end of Jan 2022, **87,292** Cyber Essentials certificates have been awarded

- The DCMS *Cyber Security Longitudinal Survey Wave 1* found that:
  a. organisations with Cyber Essentials (57%) or Cyber Essentials Plus (63%) say that their **board has received cyber security training**, compared to just 26% of those businesses who do not hold any of these certifications and;
  b. around half of businesses and charities (51% of each) have **written processes in place** (e.g. incident response plans) for managing cyber security incidents. Those businesses with Cyber Essentials (85%) and Cyber Essentials Plus (74%) are far more likely to have written processes in place.

- The Britain Thinks 2020 *Review of Cyber Essentials influence on cyber security attitudes and behaviours in UK organisations* found that:
  a. the vast majority of CE certified organisations surveyed (93%) say they are **confident they are protected against common, internet-based cyber-attacks** and;
  b. two thirds of those with CE (66%) claim that it has had a **positive impact on their ability to respond to attacks** and;
  c. the majority of certified organisations (61%) say that CE/CE+ has **reduced the likelihood of there being a significant financial cost** to their organisation in the event of a successful cyber attack.

Can requiring minimum security controls help promote best practice?

- If insurers were to require minimum security controls in order to purchase policies, this could act as a financial incentive for organisations to improve their cyber security hygiene.
- This would need to have a nuanced approach. **Cyber Essentials**, promotes a set of five basic controls which could be used for the SME market. This could help raise baseline cyber security management amongst SMEs.
- Cyber insurance could, therefore, helps companies to internalize both the benefits of good security and the costs of poor security, which in turn leads to greater investment and improvements in cyber security.

Department for
Digital, Culture,
Media & Sport

Q&A

Workshop

What role can insurance companies play in increasing cyber resilience?

Should insurance be promoting minimum standards such as Cyber Essentials?