Cyber security in the UK in 2022 - BCS Briefing

February 2022

BCS
The Chartered Institute for IT
3 Newbridge House,
Newbridge Square,
Swindon SN1 1BY
BCS is a registered charity: No 292786

The UK Government commissioned the 2022 cyber security incentives and regulation review[1] (the Review) as its previous approach to cyber security, set out in the 2016 Regulation and Incentives Review, was not delivering the necessary improvements to cyber resilience at sufficient pace and scale.

The Review identified a number of organisational barriers to effective cyber security and resilience including a lack of skills, knowledge and resources as well as a lack of sufficient incentives and regulation to encourage effective cyber risk management.

The top three key actions the UK Government is taking as a result of the Review:

- Strengthening UK cyber **legislation**, in particular through the Network and Information Systems (NIS) Regulations[2], to ensure organisations take appropriate action to secure their services[3].
- Identifying **ways in which it can mandate** large companies to appropriately assess and address the cyber risks they face
- Embedding **clear professional standards and pathways** developed by the UK Cyber Security Council[4] (UKCSC) as the professional authority

Subsequent to the Review, Government is also considering legislation to give protected status to certain cyber security professional job titles.

Other UK Government actions:

- Working with market influencers across different sectors, including insurers and procurement professionals, to ensure that awareness of cyber risk, and relevant advice and guidance, is embedded appropriately
- Increasing the provision of trusted support to advise companies on implementing technical guidance
- Identifying ways to increase the number of companies achieving the Cyber Essentials certification
- Identifying additional support for organisations to achieve a more mature level of cyber resilience such as the Cyber Assessment Framework
- Establish a cyber security baseline for critical providers of digital technology services such as managed service providers

[1] https://www.gov.uk/government/publications/2022-cyber-security-incentives-and-regulation-review
[2] https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018
[3] https://www.gov.uk/government/consultations/embedding-standards-and-pathways-across-the-cyber-profession-by-2025
[4] https://www.ukcybersecuritycouncil.org.uk/

In order to improve cyber resilience across the economy and society, the Review looks at UK Government interventions offered across four key policy areas.

Foundations

To build the foundations of cyber resilience, the government has focused on three broad areas:

1. Raising awareness of the cyber threat
2. Helping businesses know what to do (guidance, standards and frameworks)
3. Improving uptake of existing government support (engagement activity)

The Review justifies these as key areas to focus on based on earlier research conducted by DCMS that of 1.4 million UK businesses that employ staff, many still do not take basic protective actions:

- Only 15% carried out an audit of their cyber security vulnerabilities
- Only 14% train their staff on cyber security
- Only 8% of businesses have proactively sought information or guidance from government or public-sector bodies such as the National Cyber Security Centre (NCSC)
- Of those who recall government communications or guidance, just 37% report making changes to their cyber security as a direct result

The challenge therefore is to increase the reach and adoption of existing activities and guidance. The key barrier to adoption for UK organisations is the lack of commercial rationale for investment and action.

The 2019 Cyber Security Incentives and Regulations Call for Evidence[5] found that:

- two thirds of respondents believed the lack of a standardised definition of effective cyber risk management was a moderate to severe barrier to organisations effectively managing cyber risk

- The current standards and frameworks offer does not provide sufficient clarity in expectations around 'how' organisations should be thinking about their cyber risk in placing it as part of wider operational resilience and business continuity

- Improving the governance of cyber security within an organisation can often lead to the quickest improvements in overall cyber resilience

[5] https://www.gov.uk/government/publications/cyber-security-incentives-regulation-review-government-response-to-the-call-for-evidence

Capabilities

There are an estimated 134,500 individuals in the UK cyber security workforce, with around 7,500 new individuals joining each year. However, this is insufficient to supply the increasing demand for skilled candidates with an estimated annual shortfall of 10,000 individuals annually.

50% of all UK businesses (around 680,000 employers) do not have the confidence to implement the basic security controls to keep their organisation safe, in line with the requirements of Cyber Essentials.

33% of all UK businesses (around 449,000 companies) are not confident in carrying out, and do not outsource, advanced technical cyber functions such as penetration testing, forensic analysis of breaches, and security architecture.

The 2018 public consultation on Developing the UK cyber security profession indicated that the professional landscape remains complex and difficult to navigate. According to the Review there is no universally-accepted, underpinning understanding of what it means to be a cyber security professional and how to develop within a field that is made up of different specialisms and functions that range across both technical and non-technical. As a result, DCMS have funded the creation of the new UKCSC to bring structure, coherence and leadership to this space.

Market Incentives

The Review identified three main challenges relating to market incentives:

- Limited interest/awareness of cyber risk management
- Information failures relating to return on investment and likelihood of cyber attack
- Limited influence of market risk managers

Market drivers such as consumer pressure and competitive advantage could normalise investment in cyber security across the economy and compel companies to take up effective cyber risk management; these have not yet formed in many sectors or across the economy.

Organisations 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.

The government is targeting those professionals (referred to as market risk managers) who can influence and **set market expectations**, and are therefore able to stimulate demand for greater investment in cyber security across the UK economy.

As a result the UK government's focus is on:

- Continued, iterative NCSC support for Boards of Directors

- DCMS support for procurement professionals including a policy workstream on managing organisational supply chain cyber risk
- BEIS support for promotion, alignment and ongoing dialogue with IT, risk and management consultants to share learning and insights on how to incentivise board uptake of, and investment in, cyber security measures
- BEIS will build proportionate cyber security considerations into the audit and corporate reporting reform proposals
- Her Majesty's Treasury will work closely with the cyber insurance sector to explore how to make additional data available for use in modelling

The UKCSC will play a critical role in defining the skills required to perform cyber risk management in appropriate cases.

Organisations additionally face several barriers that limit their ability to prioritise **supplier and supply chain** cyber risk management, their understanding of what action to take, and their ability to act including:

- Low recognition of supplier risk
- Limited visibility into supply chains
- Insufficient expertise to evaluate supplier cyber risk
- Insufficient tools to evaluate supplier cyber risk
- Limitations to taking action due to structural imbalances

Accountability

Organisations need to do more to manage their cyber resilience with improvements still needed in a number of areas including:

- Application security
- Network security
- Supply chain risk management
- Continuity planning

There is a lack of transparency from organisations regarding their approach to cyber risk management and a contributing factor to the inadequate level of organisational cyber resilience is the lack of involvement from senior management and boards.

The UK government aims as part of wider reforms of corporate governance and reporting to drive greater accountability for and transparency of organisations' cyber resilience.