Draft version

Proposal for legislation to improve the UK's cyber resilience - 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

Table of Contents

Draft version

This document: This is a BCS briefing on the UK government's consultation[1] on a proposal for legislation to improve the UK's cyber resilience (the Consultation). This briefing does not exhaustively cover all of the Consultation, rather it provides a summary of key issues, findings and actions that are likely to be of interest to professionals working in information technology.

Executive Summary

The government has decided it needs to step in to address what it sees as the underspending on cyber security in supply chains and ensure that these systems are secure.

It has noted the growing reliance of many organisations on companies who provide important essential digital services (such as outsourcing an organisation's information technology or key business processes), often with privileged access to internal systems (collectively referred to as managed service providers).

Recent cyber incidents have demonstrated that managed service providers are key providers of digital services that expose significant systemic risks to the UK's economy and critical national infrastructure. Events such as the December 2020 SolarWinds supply chain compromise, the May 2021 ransomware attack on the US Colonial Pipeline, and the July 2021 attack on the managed service provider Kaseya demonstrate how malicious actors can compromise a country's national security and disrupt activities in the wider economy and society through supply chain attacks.

Government believes the Network and Information Systems (NIS) Regulations provides an essential mechanism for addressing such concerns. The 2020 Post-Implementation Review[2] of NIS however highlighted the need for the Regulations to better address supply chain risks. By failing to address the supply chain cyber risks associated with digital service providers, the NIS Regulations are failing to achieve their aims as envisaged. The consultation covers changes government want to make to these regulations and how in future they can be more effectively updated as necessary in response to the 2020 review.

Significant proposals being considered

The consultation proposes these additional measures for the NIS Regulations:

- Expand the scope of 'digital services ' to include 'managed services';
- Apply a two-tier supervisory regime for all digital service providers: a new proactive supervision tier for the most critical providers, alongside the existing reactive supervision tier for everyone else;
- Create new delegated powers to enable the government to update the regulations, both in terms of framework but also scope, with appropriate safeguards;
- Create a new power to bring certain organisations, ones that entities already in scope are critically dependent on, within the remit of the NIS Regulations;
- Strengthen existing incident reporting duties, currently limited to incidents that impact on service, to also include other significant incidents; and

[1] https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience

[2] https://www.gov.uk/government/publications/review-of-the-network-and-information-systems-regulations

- Extend the existing cost recovery provisions to allow regulators (for example, Ofcom, Ofgem, and the ICO) to recover the entirety of reasonable implementation costs from the companies that they regulate

This consultation is accompanied by the government consultation on embedding standards and pathways across the cyber security profession, which BCS will be responding to. A separate briefing will be available on that consultation.

Annex 1. Context and rationale for intervention

This appendix summarises key parts of the published pre-consultation Impact Assessment that are likely to be relevant for information technology professionals.

A managed service for the purposes of the consultation has been defined as a service which involves regular and ongoing service management of data, IT infrastructure, IT networks and/or IT systems, is categorised as business to business (B2B) and relies on network and information systems as a service supplied by an external, third party supplier, which involves regular and ongoing service management of IT data, infrastructure, networks and/or system. It is a business-to-business solution.

Although there is guidance available to companies through schemes such as National Cyber Security Centre's Cyber Essentials, there is currently no minimum cyber security baseline for managed service providers operating in the UK and very few mandatory cyber security requirements for companies entering this industry. Government feels managed service providers can represent a systemic risk to the UK economy and society due to the scale and concentration of services offered by the most critical managed service providers, especially those providing services to critical national infrastructure sectors.

A successful cyber attack on a managed service could affect thousands of firms, the risk created by a managed service provider's poor cyber security is much greater than the cost to their own company. This negative externality is the reason the government has decided it needs to intervene in the market and ensure that firms' systems are secure enough and that the smaller private cost of a successful breach isn't a barrier to more private investment in cyber security.

Competent authorities, the regulators that implement the regulations, require operators of essential services to secure their supply chains, primarily through contract and procurement measures , for example the Cyber Assessment Framework principle A4 for supply chains. However, the government view is that there are some entities within individual sectors that are so critical to the provision of an essential service, that relying on contractual agreements to enforce security is inadequate.

Since the creation of the NIS EU Directive in 2018, the understanding of which sectors that are essential to the UK economy are under threat has changed. A lack of regulatory oversight to ensure that these sectors are maintaining adequate cyber security protection leaves the UK open to increased cyber security risks. As a result of this government has decided to consult on changes to the NIS Regulatory framework to include new mechanisms, as outlined in the earlier section.

Annex 2. Who we are

BCS is the UK's Chartered Institute for IT. The purpose of BCS as defined by its Royal Charter is to promote and advance the education and practice of computing for the benefit of the public.

We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

As the professional membership and accreditation body for IT, we serve around 60,000 members including practitioners, businesses, academics and students, in the UK and internationally.

We also accredit the computing degree courses in over ninety universities around the UK. As a leading IT qualification body, we offer a range of widely recognised professional and end-user qualifications.