Cyber resilience of the UK's critical national infrastructure

Consultation Response – BCS, The Chartered Institute for IT

01/12/2023

Prepared by:

Claire Penketh

BCS Policy and Media Manager

BCS
The Chartered Institute for Information Technology
3 Newbridge House,
Newbridge Square,
Swindon SN1 1BY

Table of Contents

Introduction:

BCS, The Chartered Institute for IT, the professional body for technology, asked members of its Information Security Specialist Group (ISSG) for their input into the Science, Innovation and Technology Committee's call for a written response on the UK's Cyber Security Resilience: Critical National Infrastructure.

BCS held a roundtable with the following ISSG members:

- Steve Sands – BCS ISSG Chair and Information Security Consultant/Data Protection Officer at Synectics Solutions Ltd
- Wendy Goucher, Cyber Security consultant with Arcanum Cyber.
- Patrick Burgess Technical Director at Nutbourne Ltd.

These experts come from diverse professional backgrounds ranging from working on projects of national importance to start-ups and SMEs.

Executive Summary:

The ISSG welcomed the Government's focus on cybersecurity strategies and the Critical National Infrastructure (CNI). Our experts felt more attention should be paid to the private sector companies that form part of the CNI supply chain.

In addition, they would like to see a long-term strategy towards fixing the skills gap in the cybersecurity workforce.

They also highlighted issues around disseminating support and guidance information to these companies, and wanted to see more accountability at board level, along with one-stop advice and reporting portals. The group felt there should be a strong focus on areas where cyber threats most directly impact citizens and society, for example health and care.

BCS response:

1) **The strengths and weaknesses of the UK Government's National Cyber Strategy 2022 and Government Cyber Security Strategy 2022-2030 in relation to CNI for the digital economy.**

According to the BCS State of the Nation Report for 2022, the threat of a cyber attack was the leading cause of keeping business leaders and IT professionals awake at night. Key to rectifying this situation is having a skilled, competent, ethical workforce. The panel therefore agreed with the Government's emphasis within the Pillar 1 objectives of the National Cyber Security Strategy 2022 to '*enhance and expand the nation's cyber skills at every level, including through a world-class and diverse cyber profession that inspires and equips future talent.'*

Steve Sands, Chair of the BCS ISSG, said: "Strong cyber capability is essential to underpinning all aspects of technology and IT, which is necessary to deliver critical services to the nation and its citizens."

As with other areas of technology, cyber-security faces a massive skills gap. Steve said: "There needs to be a greater emphasis on increasing the number of students taking relevant cyber courses at universities and improving professional career pathways. That needs to come from Government, industry and universities."

The panel concurred with the sentiments expressed in both the UK Government's National Cyber Strategy 2022 and the Government Cyber Security Strategy 2022-2030 around *improving cyber security awareness and knowledge across all public sector workers*.

The panel said educating companies and organisations about cybersecurity risks and getting them to take it seriously was always challenging. The Chartered Institute of Information Security's (CIISec) 2022/2023 State of the Profession report stated: “71% of respondents say "people" are the biggest challenge they face in security, as the industry continues to both battle a skills shortage and to educate their colleagues."

However, a weakness in the Government's strategies could be that it doesn't completely address the need to adopt a similar awareness-raising approach aimed at the private sector, as critical government operations also depend on private contractors - see below.

2) **The effectiveness of the Government's relationships with, respectively, private-sector operators and regulators in protecting and preparing CNI organisations of most critical to the UK digital economy from cyber-attacks.**

Our experts believe the Government should strengthen partnerships, particularly between the public and private sectors, as UK CNI relies on many private-sector operators.

Whilst the Security of Network & Information Systems Regulations (NIS) imposes duties and obligations on operators of essential services (OES) and relevant digital service providers (RDSP), there is limited monitoring of the regime or operational support for operators.

Regarding monitoring, the panel felt drawing on existing structures, such as the National Cyber Security Centre (NCSC) and the UK Cyber Security Council, was essential.

There was general agreement that the Information Commissioner's Office was the body to deal with enforcing regulations. Wendy Goucher said: "There is no point in asking the government to form another body at this point; it's better to use the resources we already have."

Organisations that sit within the Government have a good understanding of cyber risk and are well supported. Private sector organisations that provide UK CNI services have business objectives which often compete with their NIS obligations.

Private sector company boards, in particular, need to be equipped to understand cyber risk, as the panel felt there is a danger of underinvestment in cyber resilience in such companies.

Boards of organisations that provide UK CNI services should be compelled to have an accountable company board member for cyber. Steve Sands said: "In the same way that you have someone in charge of finance who talks to the accountants and auditors, you would have a cyber member who would talk to their cyber teams and auditors."

Further, it should be mandatory for these organisations to report to HMG using a set of defined cyber resilience metrics to provide positive assurance of their security posture and cyber readiness.

3) **The effectiveness of the strategic lead provided by the National Security Council, Government Departments and agencies, and the National Cyber Security Centre, and the coherence of cross-government activity.**

In the case of a cyber-attack, ideally, our experts believed there should be a single mandatory reporting hub, similar to aviation, which has had Mandatory Occurrence Reporting since 1976, operated by the UK CAA.

Detection and sharing of information is often limited to HMG organisations, they said. Improved trust should be established to enable more effective sharing with those private sector organisations that provide or support UK CNI services. The panel said organisations should be compelled to share incidents (actual and near-miss) similarly to the aviation industry. Over time, this will reduce the volume and severity of incidents impacting UK CNI Services.

The panel said it was essential to achieve a balance between scaring off firms from reporting because they were afraid of the consequences, such as being fined for being negligent and using this reporting process as a means of learning lessons. Steve Sands said: "This is not about blame; it's about learning across the industry how to do things better when it comes to cyber-security."

4) **What are the interventions that are required from Government, and CNI organisations most critical to the UK digital economy to ensure the Government's cyber resilience targets by 2025 are achieved?**

The panel noted the Government's commitment in relation to CNI for understanding the risks from, for instance, external supply chains and the need for 'c*lear accountability and robust assurance (that) would ensure that risk owners are aware of the risks they have the responsibility to manage and that they are doing so appropriately*.' (Government Cyber Security Strategy 2022–2030)

The panel said cyber must be seen as a business risk rather than a technical issue; what was needed was a single government department responsible for cyber security that industry/ organisations external to the Government could contact about their concerns and for guidance.

The panel said plenty of good quality resources are available from the Government and associated bodies – but they felt there is a long-term problem in disseminating that information.

One solution proposed by the panel was a one-stop government portal where board members and the staff of companies and organisations could go for advice and guidance.

Patrick Burgess suggested that a model similar to that used by HMRC could be a good template for a single Cyber Advice Portal, signposting users to a series of links and resources, depending on the question. He said: "Someone with a question about cyber-security at their firm would fill in the details saying who they are, the size of the company, how many people in the organisation, and then 'click', you'd know what's available resource-wise to support and guide your company."

5) What role will 'secure by design' and emerging technologies play in the cyber resilience of CNI most critical to the UK digital economy and their supply chains?

Secure by design is critical to maintaining the confidentiality, integrity and availability of CNI systems and services. Several factors adversely impact the 'secure by design' objective. The panel felt significant risks to resilience were caused by the deployment of poor-quality software that lacked adequate testing. The growth of readily available open-source software (including the expected tsunami effect of automatically generated code by AI Large Language Models) exacerbated risk in this area. Other hazards include weak SDLC processes, including inappropriate use of agile principles (resulting in insecure MVP deliverables).

Regarding the Government's approach to standards and regulations for cyber resilience and preparedness, supply chain access and trusted partners, the panel said such criteria are essential to communicating and implementing 'good practice'. However, for standards to be highly effective in delivering improvement, they need to be independently assessed and certified.

In conclusion, the panel said 'secure by design' is the starting point for reducing the threat of a cyber-security attack.

About BCS
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 governments 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 Information Technology, we serve over 70,000 members, including practitioners, businesses, academics, and students, in the UK and internationally. We accredit the computing degree courses in ninety-eight universities around the UK and as a leading IT qualification body, we offer a range of widely recognised professional and end-user qualifications.