Cyber Security: critical to delivering services, safeguarding citizens, and protecting the UK economy.

Introduction

Technology underpins everything the incoming government hopes to deliver and achieve, and to protect those systems, cybersecurity must be taken more seriously. **We are calling for a compulsory, not voluntary, Governance Code of Practice for Cyber Security to be implemented.** Society and organisations in the UK increasingly depend on a complex ecosystem of IT systems and services that are often invisible until they don't work. **These systems are at significant risk from software failure and breaches**.

The government needs **to take urgent action** so cybersecurity and cyber resilience are delivered 'by default' and not considered an optional extra or something that can be retrofitted. This depends on qualified, experienced cybersecurity professionals to protect systems and build trust.

Background

According to the **National Crime Agency, the cost to the UK economy runs into billions of pounds a year**[1]. The personal impact on members of the public is huge as services such as transport or health are disrupted, as shown by the recent cyberattack on an NHS provider in London[2], which disrupted services and led to data breaches.

We are seeing **increasing numbers of outages and data breaches,** which often have a profound and lasting impact on the lives of ordinary citizens and the economy itself.

In March 2024 our response to the previous government's call for views on a draft Cyber Governance Code of Practice said it should be compulsory, not voluntary, if it were to be more effective. [3]

BCS also called for company boards to include an appropriately skilled and informed member, who along with the board will be held accountable for the firm's cybersecurity throughout its life cycle.

In the same way we have **health and safety standards,** we need easily accessible, understandable cybersecurity processes and strong governance.

BCS' Digital and Business Life report 2023 [4] found the **threat of a cyber attack** was the leading issue that kept CEOs and IT professionals awake at night.

The latest official Cyber Security Breaches Survey [5] show *'half of businesses and around a third of charities in the UK report having experienced some form of cyber security breach or attack in the last 12 months.'*

Steve Sands Chair of the BCS Information Security Specialist Group (ISSG) said: "**Step One** is to **protect** your systems and data from cyber attacks."

"Step Two is to ensure adequate **respond and recover processes to restore services quickly and limit disruption**. This can't happen if you don't have reliable backups."

[1] https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime
[2] https://www.bbc.co.uk/news/articles/c9ww90j9dj8o
[3] https://www.bcs.org/media/kpqpbpws/cyber-security-code-of-practice-response.pdf
[4] https://www.bcs.org/policy-and-influence/tech-and-society/digital-in-business-life-report-2023-security-professionalism-and-priorities-for-2023/what-keeps-you-up-at-night/
[5] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

Cyber Security: critical to delivering services, safeguarding citizens, and protecting the UK economy.

Recommendations

- Introduce a **Cybersecurity Code of Practice with mandatory breach reporting** and quarterly reporting on risk (including third-party risk) rather than a voluntary code, as currently.
- **Require company boards** to include a member who will be **held accountable** for the firm's cybersecurity throughout its life cycle.
- Enforce a **'secure and resilient by design' culture** for all critical and vital IT systems.
- **Build strong cyber governance within organisations**, including continuous monitoring/assurance of third parties, especially in government and Critical National Infrastructure supply chains.
- Ensure cyber resilience is built into business resilience plans, with improved systems in place to restore critical systems quickly.
- Government and industry to **work together to support professional registrations and Chartered status for cyber security practitioners,** to build public trust and confidence at governance level.
- Invest **more in training** for the cyber workforce to produce highly skilled, ethical competent cyber professionals.

Recommendations cont.

- Develop an **ongoing government-led awareness-raising campaign** on cyber-security and cyber resilience, backed by industry partners.
- Set up an **easily accessible one-stop** shop on gov.uk for SMEs need to meet all their cybersecurity information and advice needs.

Conclusion

Strengthening government policy, with a mandatory code of practice, organisational culture and professional standards in cybersecurity will:

Secure our critical national infrastructure and the important IT systems delivered by businesses across all sectors.

This will protect the UK economy, ensure our competitiveness and credibility as a global partner and ensure the safety of society at large.