Cyber Security and Resilience Bill Position Paper

About the Institution of Engineering and Technology (IET)

The IET is a trusted adviser of independent, impartial, evidence-based engineering and technology expertise. We are a registered charity and one of the world's leading professional societies for the engineering and technology community with over 158,000 members worldwide in 148 countries. Our strength is in working collaboratively with government, industry and academia to engineer solutions for our greatest societal challenges. We believe that professional guidance, especially in highly technological areas, is critical to good policy making.

Executive Summary

The Cyber Security and Resilience Bill (CSRB) is a welcome step forward to bolster cyber defences in UK businesses and the public sector, bringing together the current piecemeal regulatory frameworks. There are going to be key areas that will be critical to the successful implementation of the Bill, including, increasing the remit and scope of the CSRB, ensuring robust professional standards, focussing on response as well as preparation for cyber-attack and ensuring clarity and proportionality.

Key Messages

- **Remit:** The remit of sectors covered by the CSRB is too narrow to adequately protect the economy and provide resilience to the UK, for example food and medical manufacturing should be covered. The Bill should be strengthened and align more closely with European legislation, particularly for critical infrastructure.

- **Standards:** There should be standardisation across regulators to ensure that there is parity when considering an appropriate implementation of the bill between sectors.

- **Clarity and Proportionality:** Clarity and guidance on what is expected of business and repercussions for breaching the Bill is needed to ensure smooth compliance and support business continuity. Proportionality must be a key aim.

- **Response plans:** Stronger requirements for response plans, underpinned by standards, are required. Cyber security is not just about prevention, but businesses should model their response in the event of a breach to identify weaknesses as a part of routine response planning.

- **Professionalism:** Cyber security threats are ever evolving, which is why cyber security experts should be chartered and backed by professional organisations to share best practice.

- **Mandatory Reporting:** The IET welcomes the mandatory reporting outlined in the Bill, however we must ensure that minimises additional burden to businesses, particularly when reporting is duplicated across multiple organisations.

Background

According to research by ESET, cyberattacks cost UK businesses an estimated £64 billion annually, with £37.3 billion in direct costs and £26.7 billion in indirect costs (ESET, The True

Cost of Cyber Attacks: Balancing business protection and risk). In the case of the ransomware attack at M&S, it was announced in November that their pre-tax profits decreased from £391.9m to £3.4m, a 99% shortfall (BBC, M&S profits almost wiped out after cyber hack left shelves empty). With 90% of large organisations and 74% of SMEs reporting information breaches in 2024, cyber security is more important than ever (Barclay Simpson, calculating the 2 reputational cost of cyber security breaches). These figures pose a significant risk to businesses which could stifle growth. It is also important to ensure that supply chains are protected, as this can have a knock-on impact for larger businesses and both the local and national economy.

Attacks on public services can have an impact that goes beyond financial to life threatening. In June 2024, a cyber-attack on a supplier of pathology services to the NHS in south-east London led to two NHS foundation trusts postponing 10,152 acute outpatient appointments and 1,710 elective procedures (National Audit Office, Cyber threat to UK government is severe and advancing quickly, spending watchdog finds). **Having the relevant skills are one of the biggest ways to protect against attack however cyber security threats are ever evolving and that is why to ensure the success of this legislation, businesses should be supported by cyber security experts, backed by professional organisations.**

Remit

Although priority sectors will be expanded from the NIS regulation, the IET is still concerned that the remit is too narrow to adequately protect the UK's vital services and economy, particularly given the extensive impact recent cyber breaches have had on supply chains. For example, the Cyber Monitoring Centre reported that the JLR breach alone had an estimated £1.9 billion impact on the UK economy (Reuters, Jaguar Land Rover hack cost UK economy an estimated $2.5 billion, report says). There are key sectors that should be included as a priority now, for example, food and medical supplies however there should also be flexibility to update the Bill when necessary to include other sectors.

There is significant overlap between sectors and regulators within the scope of cyber security therefore there needs to be a systems approach to applying the legislation once it passes through parliament. It is clear that the CSRB needs strengthening in key areas, for example, greater coverage of critical sectors, in line, but not limited to European legislation (NIS2) which "covers connected objects in the home, hospitals, energy grids and railways, with focus on Cross-border Security Operations Centres to procure cyber threat detection tools and services...this highlights the need for optimised security controls" (UK Cyber Security Council, Cyber Insurance - A Digital Decade).

One example is that energy infrastructure outages can have widespread and serious consequences for both individuals and society. The risk of energy infrastructure failing due to cyber security attacks can be significant. With an increase in the number of devices connected by digital networks, including in energy infrastructure, it exposes the grid to new risks. Energy outages then have knock on effects for other sectors, such as health, transport and food. There needs to be a technical understanding of the issues, processes, and interdependencies when assessing risks with a whole-system engineering perspective informing decisions.

The Bill focuses primarily on post-cyber-attack activity, which is a welcome step in supporting regulators and affected sectors to design and implement resilience mechanisms, including clear reporting lines for breaches with significant impact. However, additional requirements should be applied to sectors that rely on non-UK domestic products, enabling regulators to

link accountability to existing civil law frameworks or, where appropriate, the Computer Misuse Act 1990.

Role of regulators

There is a need for clarity and parity across regulators with regards to application of the new rules. Furthermore, businesses will need to be clear on how they should comply, particularly which businesses are within scope. Although regulators will be placed on a stronger footing there are still a large number of regulators across sectors, with many overlapping in the event of a singular incident. **Clear standards should be set to ensure there is parity on the 'adequacy' of measures outlined in the Bill and proportionality for any breaches.** Playbooks on best practice should be developed which transcend regulators.

The Governments Cyber Action Plan published on 6th Jan 2026 is to be commended for giving direction to Public Sectors (Gov.UK, Government Cyber Action Plan), however the Bill should either refer to it, or provide an alternate version applying the Cyber Bill to the Private Sector.

Additionally, at present, international vendors dominate cyber security certification frameworks, creating a fragmented understanding of what "good" cyber security skills look like. The need for a UK-defined minimum standard is further reinforced by the introduction, from 2026, of Standard Operational Classification (SOC) code 2135 (Cyber Security Professionals) under the Skilled Worker visa route (Gov.UK, Skilled Worker visa: eligible occupations). While this change is welcome, the Bill has a critical opportunity to provide a joined-up framework for UK private standards, regulation, workforce requirements, and skills development. Failing to do so would be a missed opportunity to embed digital sovereignty within the UK's national cyber security posture in terms of cyber fraud and cyber crime.

Proportionality, cost and standards

Although Cyber Essentials is a welcome resource and standard for the sector, it should be considered the bare minimum standard of cyber security protection that a business should have, and this should not be seen as tick box exercise, but **businesses should strive to adapt to continual innovations in this area of technology**. Stronger requirements for response plans, underpinned by standards, are required. Cyber security is not just about prevention, but businesses should model their response in the event of a breach to identify weaknesses as a part of routine response planning. **Policy makers must be cautious that the CRSB does not incentivise rising costs for cyber security whilst still delivering the minimum standard.** Even basic cyber security measures can be costly, but the cost of a breach can be much greater, however this is a greater barrier for smaller businesses than larger ones.

The rising cost of cyber security insurance is also a concern, however the CSRB may help to provide structure and guidelines for businesses to ensure that their protocols are clear, for example evidencing why certain measures are in place and that best practice has been embedded throughout the organisation. Government estimates that 20% of businesses and 14% of charities have been the victim of at least one cybercrime in 2025 (Gov.UK, Cyber security breaches survey 2025). Furthermore, they can demonstrate that they are constantly evolving their strategy to protect themselves against new threats by being professionally registered (UK Cyber Security Council, Cyber Insurance - A Digital Decade).

Professionalism and skills

We must be mindful of the rapidly evolving nature of cyber security threats. **The IET 2025 skills survey showed that cyber security skills were most sought after by businesses (38%) in the next five years** (IET, UK Engineering and Technology Skills). It is critical that cyber security measures are led by chartered experts, backed by professional organisations to ensure a high level of competency.

There is a notable shortage of skilled cyber security professionals worldwide which leaves organisations vulnerable to cyber threats and data breaches. It is estimated there is a shortfall of over 173,000 workers in the STEM sector: an average of 10 unfilled roles per business in the UK, which is costing the economy a staggering £1.5bn per annum (IET, Government urged to tackle £1.5bn engineering skills shortage through primary and secondary education drive). **Shockingly, 76% of employers in the IET 2025 skills survey report that they struggle to recruit for certain skills, with 17% highlighting cyber security** (IET, UK Engineering and Technology Skills).

Training costs for cyber security professionals can vary widely depending on the level and type of training. Costs can also vary depending on the standard of the qualification - whether it be a basic certification course, more advanced course, undergraduate or post-graduate degree. For example, entry-level certifications like CompTIA Security+ might cost around £400, while undertaking an undergraduate then postgraduate degree course would cost over £40,000. Investing in good training for cyber security professionals is crucial, as it can significantly enhance an organisation's ability to protect its data effectively. **Chartership is the gold standard to ensure a high level of competency in this field**.

Whilst the CSRB brings all Critical National Infrastructure (CNI) sectors into scope and brings providers to rely on baseline guidance such as Cyber Essentials, it should also take the opportunity to create and mandate a 'National Cyber Security Apprenticeship Programme' aligned to the UK Cyber Security Council's professional development pathways. At a minimum, the Bill should require a recognised UK skills standard, such as the Associate Cyber Security Professional (ACSP) designation (UK Cyber Security Council, Professional Cyber Security Titles).

In addition, regularly updating skills and knowledge for all employees through continued education and training is also important given the rapidly evolving nature of cyber threats. Workers in the STEM sector are in high demand, but **we do not have the current pipeline of engineers and technicians with the right skills to fill the labour market – something we have been reporting via our skills survey for the last 20 years, and frustratingly nothing has changed in that time** (IET, IET responds to UK Government signalling move to curb overseas hiring for tech and engineering jobs).

Once the CSRB has passed, a series of competency frameworks should be developed and to ensure that when new products come to market, practitioners are able to still use these while working within the legislation. These engineering patterns (reusable solutions to common problems) can support best practice by creating rules for products that are yet to come to market.