Supplementary written evidence submitted by NCC Group to the Cyber Security and Resilience (Network and Information Systems) Public Bill Committee (CSRB29)

Introduction

- As the UK's first ever law with 'cyber security' in its title, the Cyber Security and Resilience (CSR) Bill will be **essential for bringing the cyber rules governing critical infrastructure in line with modern threats, economic realities and technological developments**. It also retains crucial flexibility to keep pace with the ever-changing cyber landscape.
- However, as covered in this submission and our Chief Scientist Chris Anley's oral evidence[1], **it must not be seen as a silver bullet**. Through our work supporting UK and global organisations to enhance their cyber resilience and comply with emerging cyber regulations, we see the firsthand how the escalating rate, severity and sophistication of cyber threats requires a genuinely 'whole-of-economy' response.
- There are still **important questions around incentivising secure technology development, uplifting economy-wide cyber resilience, and modernising the UK's cybercrime laws**. There is also further work to be done on the **detail underpinning the Bill** to ensure it is an effective piece of legislation.
- We explore these points in more detail below.

About NCC Group

We trace our origins back to Harold Wilson's famous 1963 "White Heat of Technology" speech in which he committed to produce more computer scientists to keep pace with technological change. The creation of the "National Computing Centre" was one of the visible outcomes of the speech. Following a management buyout in 1999, NCC Group was born. We have since grown into a global powerhouse, unique in our position on the London Stock Exchange as a large-scale cyber services company and with a presence across Europe, North America and Asia Pacific. We remain driven by our purpose to create a more secure digital future and provide high-quality, highly-skilled jobs to over 1,000 UK colleagues, with double that number of employees worldwide.

We are extremely proud of the critical role we play in enabling UK plc to thrive – whether it's enhancing the digital resilience of critical infrastructure, supporting the British Library to respond to and recover from its significant cyberattack or helping dozens of local authorities to rapidly improve their cyber resilience in the wake of the COVID-19 ransomware threat.

1. Consulting early on secondary legislation and guidance

Much of the detail underpinning the implementation of this legislation will be set out in secondary legislation and guidance. We broadly agree with this approach, given the fast-

[1] https://hansard.parliament.uk/Commons/2026-02-03/debates/12f8b501-16c6-476b-bc85-035092381c43/CyberSecurityAndResilience(NetworkAndInformationSystems)Bill(FirstSitting)

moving and ever-evolving nature of cyber security requires a degree of flexibility in how the law is implemented.

That said, the draft secondary legislation and guidance is yet to be published, making it difficult to effectively scrutinise some parts of the primary legislation. We therefore **back wider industry calls for the Government to consult as soon as possible on the draft secondary legislation and guidance**, enabling a full understanding of how the new law will work in practice.

Two key areas demonstrate this point – placing responsibility on senior leaders and incident reporting thresholds:

a) Senior leader responsibilities

Effective implementation of the CSR Bill will require senior leaders' buy-in at the organisations set to be regulated under the new regime. Delivering the levels of cyber resilience the NIS regulations demand requires strategic prioritisation and investment – much of which will be driven from the board-level down.

Other jurisdictions have sought to achieve senior leader buy-in by placing specific responsibility and, sometimes, legal liability on leaders to comply with cyber rules. For example, the EU's NIS2 places specific and individual responsibility and liability on senior leaders to approve, oversee and ensure implementation of cybersecurity risk management measures, as well as undergo training themselves. Consequences for noncompliance can include fines and suspensions from managerial positions.

We welcome Minister Kanishka Narayan MP's commitment to "ensure that specified security and resilience activities, including the possibility of specific responsibilities [for boards], are set out very clearly"[2]. Indeed, we understand that the Cyber Governance Code of Practice, which is aimed at boards, may be incorporated into secondary legislation for the CSR Bill. That said, as the detailed requirements of the CSR Bill are yet to be published, **we continue to lack clarity on if and how the Government intend to place responsibility for compliance on senior leaders**. Understanding whether this is indeed the case would enable Parliament, industry and the wider cyber ecosystem to assess the appropriateness of the primary legislation – or whether further amendments are needed related to senior leaders' obligations.

b) Incident reporting thresholds

The CSR Bill introduces a new definition of the cyber incidents that will need to be reported, to include events having, or being *capable of* having, an actual adverse effect on the operation or security of network and information systems.

As raised by several witnesses during the Committee hearings, the **thresholds for which incidents meet the new lowered "capable of" definition must be carefully considered and clearly defined for each sector regulated under NIS**. Too few details could lead to significant overreporting, overwhelming both businesses and regulators. Understanding these

[2] https://hansard.parliament.uk/Commons/2026-02-03/debates/9a3f1e53-d0e0-41d6-9c01-d316f78a8b4f/CyberSecurityAndResilience(NetworkAndInformationSystems)Bill(SecondSitting)

thresholds – or, at the very least, how they will be set – is essential for understanding whether the new definition of reportable incidents is legally appropriate.

2. Simple and effective incident reporting

While greater reporting of cyber incidents is welcome (not least because it will help Government understand the true scale of the threats facing the UK), **the current landscape of reporting rules is unnecessarily complex**.

As well as the NIS incident reporting rules that will be strengthened by the CSR Bill, organisations also face GDPR data breach obligations, sector-specific regulations (e.g. for telecoms) and, soon, economy-wide Home Office rules requiring all UK organisations to report ransomware attacks. **Across these requirements, there are notable differences** in the types of incidents that need to be reported, the body that the report needs to be made to, and the reporting timelines. There are also multiple voluntary reporting mechanisms through Report Fraud, the National Cyber Security Centre (NCSC) and law enforcement.

The first few hours and days of a cyber incident can be incredibly complex, confusing and stressful for organisations. Having multiple overlapping and, sometimes, conflicting regimes only serves to create confusion, further regulatory burdens and hamper growth, without the net benefits to national security.

We urge the Government to **implement a unified approach to reporting**, with one single point of contact and timelines that align across regulatory regimes. Facing similar challenges, the Australian Government recently introduced a single reporting portal[3] for all cyber regulatory requirements, while the European Commission has announced plans to introduce a unified reporting platform through which entities can simultaneously fulfil their incident reporting obligations under multiple legal acts[4].

3. Building cyber resilience across the entire economy

Cyber security is economic security. The UK's Industrial Strategy recognises that sustainable and secure growth requires strong levels of cyber resilience across the economy. Recent unprecedented incidents impacting British institutions have shown just how true this is.

The cyber attack on Jaguar Land Rover (JLR) has been reported to be the costliest cyber incident in UK history, with the Cyber Monitoring Centre (CMC) estimating the damage to be in the range of £1.6bn and £2.1bn, split between JLR and its supply chain[5]. Research from the UK Government's CSR Bill press release states that the **average cost of a significant cyber-attack in the UK is now over £190,000**. This amounts to around **£14.7 billion a year across the economy** - equivalent to 0.5% of the UK's GDP[6].

---

[3] https://www.cyber.gov.au/report-and-recover/single-reporting-portal
[4] https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal
[5] https://www.bbc.co.uk/news/articles/cy9pdld4y81o#:~:text=The%20cyber%20attack%20on%20Jaguar,UK%20history%2C%20according%20to%20researchers.
[6] https://www.gov.uk/government/news/tough-new-laws-to-strengthen-the-uks-defences-against-cyber-attacks-on-nhs-transport-and-energy

But, **many of the most impactful incidents in the UK in recent years have had real-world consequences for organisations that will <u>not</u> be directly impacted by the Bill**. Based on the Government's and regulators' Impact Assessments[7], we estimate that **legally mandated cyber security requirements will apply to only 0.1% of UK businesses**, even after the introduction of the UK Cyber Security and Resilience Bill. Meanwhile, the World Economic Forum's Global Cybersecurity Outlook 2026[8] finds that three quarters of business leaders have a positive view of the effectiveness of cyber regulations, with 58% noting that these regulations help CISOs raise cybersecurity awareness at the board level and 55% highlighting how such rules drive tangible improvements in overall security posture. While we must avoid overregulating, the positive role such requirements can play across the economy should be considered.

In addition, **SMEs** – the backbone of the UK's economy making up 99.8% of the total business population – **often lack the skills and budgets to implement proportionate cyber protections**, leaving them particularly exposed. A recent government-commissioned report[9] found:

> *"Many SMEs have minimal cyber security budgets and potentially face severe financial impacts, such as lost revenue and extended recovery times, if they suffer a cyber-attack. This vulnerability is further compounded by interconnected supply chains, where a breach in one SME can affect larger networks."*

The UK must take a 'whole of economy' approach to cyber security, ensuring that resilience measures are not only targeted at critical services, but tailored to other essential parts of the UK economy. In practice, this must include:

- **Working with technology providers to embed secure-by-design and secure-by-default principles in their products** and software – particularly those most relied upon by UK businesses. In practice, this may require implementing proportionate, economy-wide legislation mandating minimum security requirements – akin to the EU's Cyber Resilience Act, and the requirements set out in the (currently voluntary) Software Security Code of Practice.

- **A digital safety net for SMEs –** a nationwide 'first responder' service that provides proportionate (free-at-the-point-of-use) support to small businesses that have been victims of a cyberattack. It is our view that it is unrealistic to expect small organisations to adhere to – and invest in – the same cyber resilience standards as larger firms. Therefore, we must consider how we can prevent smaller organisations from failing in the event of a cyberattack. In a similar move, the Australian Government is investing $8.1 million over 3 years to provide free, person-to-person support for small businesses during and after a cyberattack[10].

---

[7] Total UK business population is 5,496,050: https://www.gov.uk/government/statistics/business-population-estimates-2024/business-population-estimates-for-the-uk-and-regions-2024-statistical-release. Estimated total of organisations regulated under NIS regulations, CSR Bill, PRA regulation, TSA and PSTI Act is 7,332: https://publications.parliament.uk/pa/bills/cbill/59-01/0329/impact_assessment.pdf; https://assets.publishing.service.gov.uk/media/5fb7d4f2d3bf7f573228a3a3/FINAL_The_Telecommunications_Security_Bill_2020__The_Telecoms_Security_legislation_-_Acc.pdf; https://www.bankofengland.co.uk/prudential-regulation/authorisations/which-firms-does-the-pra-regulate#:~:text=The%20Prudential%20Regulation%20Authority%20regulates,lists%20of%20these%20firms%20here; https://assets.publishing.service.gov.uk/media/627a7730d3bf7f5c05c3eee0/Impact_Assessment.pdf

[8] https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

[9] https://assets.publishing.service.gov.uk/media/6891e704f15b237bf6610956/Insuring_Resilience_-_The_state_of_SME_cyber_insurance.pdf

[10] https://ministers.treasury.gov.au/ministers/julie-collins-2022/media-releases/more-support-help-small-business-cyber-resilience

4. Providing stronger legal protections for cyber security professionals

The UK's **outdated cybercrime law – the Computer Misuse Act 1990** – inadvertently criminalises some forms of cyber security research, holding back sovereign capabilities that are necessary to counter 21st century cyber threats. The introduction of the Cyber Security and Resilience Bill to Parliament presents a **perfect opportunity to update this 35-year-old legal framework**, ensuring UK firms can effectively combat cyber threats and comply with the regulatory obligations set out in the Bill.

Written at a time when **only 0.5% of the public had access to the internet**, the Computer Misuse Act's blanket prohibition of all unauthorised access to computer systems fails to distinguish between malicious attackers and cyber security professionals acting in the public interest. This has resulted in security professionals operating with one hand tied behind their back against a fast-evolving threat landscape, **hampering national security and innovation**. The UK Home Office's own call for evidence found[11] that **two-thirds** of respondents believed the **current Act does not provide sufficient protection** for legitimate cyber security activity.

As founding members of the CyberUp Campaign[12], we join others across industry, academia and the cyber ecosystem[13] in sharing a common belief: **the UK's cybercrime laws should not inadvertently criminalise the very same people seeking to keep the nation safe and secure**. In practice, we advocate for the **inclusion of a statutory defence** in the Act that would give individuals across the cyber industry legal protections to carry out crucial vulnerability research and threat intelligence, provided they meet certain safeguard criteria[14]. Done right, this reform will **empower cyber professionals to develop key capabilities, fight cybercrime more effectively and bolster national security.**

We welcome recent commitments from the Government to progress policy work on a legal statutory defence for industry[15]. However, concrete steps are yet to be laid out, and other countries are forging ahead with their own reforms[16]. **The UK is in danger of being left behind.**

We ask that the Committee table the CyberUp Campaign's amendment that has been drafted in consultation with legal experts and would enact necessary updates to the Computer Misuse Act:

Definition of unauthorised access to computer programs or data

In section 17 of the Computer Misuse Act 1990, at the end of subsection (5) insert—

"(c) he does not reasonably believe that the person entitled to control access of the kind in question to the program or data would have consented to that access if he had

---

[11] https://www.whatdotheyknow.com/request/foi_request_into_computer_misuse/response/1843896/attach/html/3/FOI 65005 Eleanor Brady FINAL.pdf.html
[12] https://www.cyberupcampaign.com/
[13] Computer Misuse Act reform is backed by major industry leaders including BT and NCC Group, professional bodies like CREST and Cyber Scheme, trade associations such as techUK, legal academics the Criminal Law Reform Now Network (CLRNN) and the ICO.
[14] https://www.cyberupcampaign.com/news/a-proposal-for-a-principles-based-framework-for-the-application-of-a-statutory-defence-under-a-reformed-computer-misuse-act
[15] https://www.gov.uk/government/speeches/keynote-address-to-ft-cyber-resilience-summit-2025
[16] The EU's Cyber Resilience Act encourages Member States to adopt measures that ensure cyber professionals are not prosecuted or held liable for researching vulnerabilities, with Germany, Portugal and Malta among the EU countries moving forward with these much-needed updates. The US, Belgium, the Netherlands and France already have more permissive legal regimes, while Australia recently consulted on its own updates.

known about the access and the circumstances of it, including the reasons for seeking it;

(d) he is not empowered by an enactment, by a rule of law, or by the order of a court or tribunal to access of the kind in question to the program or data."

Defences to charges under the Computer Misuse Act 1990

(1) The Computer Misuse Act 1990 is amended as follows.

(2) In section 1, after subsection (2) insert—

"(2A) It is a defence to a charge under subsection (1) to prove that—

(a) the person's actions were necessary for the detection or prevention of crime; or

(b) the person's actions were justified as being in the public interest."

(3) In section 3, after subsection (5) insert—

"(5A) It is a defence to a charge under subsection (1) to prove that—

(a) the person's actions were necessary for the detection or prevention of crime; or

(b) the person's actions were justified as being in the public interest."

February 2026