Cyber Security and Resilience (Network and Information Systems) Bill Committee Submission

February 2026

Executive summary

1. Cyber insurance is one the fastest growing product lines in the UK's world leading and innovative insurance industry, and our industry is well placed to address cyber risks and convene stakeholders to collectively improve the UK's cyber resilience.
2. Cyber risks, and especially ransomware, have been identified as top economic threats, as demonstrated by cyber-attacks on leading UK businesses, including M&S, Co-op, Harrods and Jaguar Land Rover.
3. We want to work with the government on our proposal to develop a strategic dialogue to clarify and align the expectations across businesses, insurers and the government to explore how best to work together to manage cyber risk and strengthen national cyber resilience.
4. We welcome the Cyber Security and Resilience Bill and the government's focus on strengthening the resilience of the UK's essential services and their supply chains against cyber-attacks through widening the scope of the Network and Information Systems (NIS) Regulations.
5. The Bill has the potential to benefit the entire economy by enhancing cybersecurity and improving resilience across a wide range of organisations. We believe that the industry has a role to play in supporting this goal.
6. While the Bill rightly addresses gaps in our Critical National Infrastructure's (CNI) cybersecurity, we also must address the cyber resilience of Small- and Medium-sized Enterprises (SMEs).
7. We support the government's proposal to introduce a mandatory cyber incident reporting regime for essential services and their supply chains to provide a clearer picture of the threat landscape.
8. We welcome, and strongly support, the government's ambitions to simplify and streamline regulation. It's important that the Bill's reporting requirements don't contradict the government's pledges to reduce regulation and duplication, especially as the financial services regulators develop their regime to regulate Critical Third Parties.
9. Clear guidance on what to report and when must be published in a timely manner to help regulated entities comply with the new regulations, as well as adopting a proportional approach, to ensure that requirements do not become overburdensome on SMEs.

Key asks for our sector

10. Continue to work with our sector to develop our proposal on a strategic dialogue to clarify and align the expectations across businesses, insurers and the government to explore how best to work together to manage cyber risk and strengthen national cyber resilience.
11. Clearly delineate the responsibilities of businesses, insurance, and government in cyber security and understand where the industry can and cannot support these goals.
12. Work with our sector to raise awareness of the value of cyber insurance and address the cyber resilience of SMEs.

13. Set out clear, objective definitions for who will be in scope of the Bill – specifically whether financial services institutions who operate their own data centres will be drawn into the scope of the NIS Regulations.
14. Clear and timely guidance for firms under the Bill's scope to help with compliance.
15. Ensure the reporting requirements set out in the Bill don't contradict the government's pledges to reduce regulation, duplication and costs for businesses and set out further detail on the exemption for small and micro-sized businesses.
16. Consider the appropriateness of the 24-hour and 72-hour timelines for reporting generally, and whether a tiered approach could be pursued for smaller regulated entities, which are less likely to have the capacity and in-house expertise to produce the reports on time.

Cyber insurance

17. Cyber insurance is a relatively new product, but it has matured in recent years, reflected by improved underwriting discipline, more clarity in policy wordings, and a better understanding of the overall risk landscape.
18. Cyber insurance is more than just an indemnity product that helps you to cover the costs of a malicious cyber incident or system outage. It offers proactive and reactive services to improve cybersecurity, detect issues early, prevent cyber-attacks from happening, and respond and recover if the worst happens. This service provision is a key driver of resilience.
19. Both the global and UK cyber insurance markets have grown at more than 20% per annum, with the UK market being forecasted to reach between £1.3 billion and £1.5 billion by 2027.
20. Last year, insurers paid out £197 million to help businesses recover from cyber incidents. Our data shows a 230% year-on-year increase in the amount paid to support businesses with cyber-attacks, £138 million more than in 2023.
21. Recent incidents affecting M&S, Co-op, Harrods, and Jaguar Land Rover highlight the growing need to focus on the expectations and responsibilities of larger businesses. These firms are not only major employers and economic anchors, but also nodes in complex supply chains, meaning their resilience has far-reaching implications. The increasing reliance on critical vendors and suppliers, such as cloud infrastructure and software providers, is driving a concentration of risk across the wider economy.
22. Despite these recent major cyber-attacks, insurers are still keen to provide cover to more UK organisations, from SMEs to multinationals, and in 2025, we continued to see excess capacity in the market.
23. We're working with the London Market Association and BIBA to create a template cyber insurance wording and underwriting glossary of commonly used cyber terminology in partnership with insurers and regulators to help increase understanding of what cyber insurance can offer.
24. **We've proposed the government establishes a strategic forum to clarify and align expectations across large businesses, insurers and government to explore how best to work together to manage cyber risk and establish a framework to strengthen national cyber resilience.**

SMEs

25. While the Bill rightly focuses on building the resilience of our critical national infrastructure, more must be done to address the cyber resilience of Small and Medium-sized Enterprises (SMEs).

26. The take up of cyber insurance by UK SMEs is very low. Different methods are used to calculate insurance penetration, but reliable estimates can vary and range from 10%-40%. Last year, we published our Cyber Resilience for SMEs: The Insurance Gap Explored report, exploring how cyber insurance can help to prevent and alleviate the impact of cyber-attacks for SMEs. As recommended in our report, we want to work with the government to raise awareness of the value cyber insurance offers, both in helping to improve businesses' cyber defences and to help them withstand and survive a cyber-attack.
27. Our Cyber Safety Tool, a free, interactive tool also helps SMEs assess their own cyber security and plug any identified gaps in their cyber resilience. Our Cyber Safety Tool has been created using expertise from within the insurance industry and utilises identified best practice and protocols from the National Cyber Security Centre (NCSC).
28. As cyber risks continue to grow, SMEs are typically more vulnerable and less well placed than larger businesses to respond to cyber threats, generally due to overstretched resources, including IT and potential security gaps.
29. Only 25% of medium-sized businesses, according to research by Public First and the ABI, hold cyber insurance cover. 57% of respondents to the survey have software or cloud services, but only 29% have cyber insurance protection. For SMEs with a physical premises, of those who have software or cloud services, 32% have cyber insurance protection.
30. Our report, commissioned by the ABI with Public First, Small Business, Big Risk: Tackling SME Underinsurance, explores the uninsurance and underinsurance of SMEs setting out the industry's commitment to increasing SME's resilience alongside a guide for SMEs explaining insurance products, how to find the right products for their business, and the value of insurance.

Scope

31. The Bill significantly expands the scope of the Network and Information Systems (NIS) Regulations, resulting in more organisations having increased duties placed on them, including those likely to already have cyber insurance (such as cybersecurity and IT vendors), and potentially insurers. Provisions to designate organisations as critical suppliers also expand the scope of the regulations further.
32. The expansion of the regulations could mean cyber insurers or their supply chains come into the scope of regulation as operators of data centres or as providers of digital services such as continuous threat monitoring and other cybersecurity services. Insurers could potentially have a role to play in helping customers and designated critical suppliers to comply with the new duties, especially smaller organisations.
33. The Bill also updates existing duties for Relevant Digital Service Providers and makes equivalent provisions for Relevant Managed Service Provides and data centre operators to provide information to their regulators at the point of registration or designation. Insurers may want to help smaller providers by providing information on the new requirements to avoid potential fines for non-compliance.
34. The cost recovery framework for regulators to recover potential costs incurred in carrying out their new duties set out in the Bill will incur additional costs for businesses and organisations. Through imposing additional costs on businesses at a challenging time this measure could potentially deter organisations from taking out a cyber insurance policy in the first place, and lead to some opting not to renew their cyber insurance policy and spend less on other wider resilience measures.

35. If insurers are captured in the scope of the Bill, costs of compliance with the regulations would ultimately filter down to SME policyholders, who are already price sensitive.
36. **We want to see clearer objective definitions for firms the Bill brings under its scope. While we appreciate this would likely become clearer as the Bill undergoes further scrutiny, certainty is needed to help support businesses in future decision making and budget planning.**

Reporting

37. We support the proposals within the Bill to introduce a mandatory cyber incident reporting regime for essential services and their supply chains. There's strong value in the government collating and publishing information about cyber incidents, potentially through an anonymised cyber incident database or exchange platform, which could help to provide a clearer picture of the threat landscape and boost cyber resilience across the UK's economy.
38. We welcome confirmation from the government that micro and small enterprises are exempt from the reporting requirements and small digital service providers can only be regulated if they are designated as a critical supplier in rare circumstances.
39. **We remain concerned about the feasibility for smaller organisations to meet the proposed two-stage reporting structure for cyber incidents as set out in the Bill, particularly requiring a full report to the relevant regulator and the NCSC within 72 hours.** While this would be feasible for larger organisations, this would not be the case for smaller supply chain companies and firms including smaller Managed Service Providers (MSPs) and critical suppliers, especially when investigations rely on external IT providers **We want to see greater proportionality on these reporting requirements, with extended timelines or even an exemption for some smaller firms.** The reporting requirements could place further strain on outsourced IT and cybersecurity providers, who would likely be required to carry out potential investigations into incidents and prepare reports for multiple regulators on behalf of their smaller clients.
40. We would like to see clearer guidelines on what to report, and when, in recognition of the potential for the lack of cybersecurity expertise among businesses. Without appropriate guidance, businesses may have concerns about data privacy and be confused by the complexity of reporting thresholds.
41. The Bill requires the Secretary of State to produce a report at least every 5 years on how the legislation has been implemented, including exploring how the legislative objectives can be achieved in a less onerous regulatory provision. We recommend that these reviews are conducted on a more regular and timelier basis.
42. We welcome the publication of the government's Regulation Action Plan and support its wider ambitions to streamline regulation. It's important that these reporting requirements in the Cyber Security and Resilience Bill don't contradict the government's pledges to reduce regulation and duplication. The Financial Conduct Authority and the Bank of England will be shortly consulting on the regulation of Critical Third Parties, in parallel with the European Union's Digital Operational Resilience Act 2025 (DORA). Streamlined structures and coordination between the government and regulators are necessary to avoid conflicting requirements and ensure effective resource allocation for intelligence agencies.

Ransomware

43. Ransomware is fast becoming the key cyber threat facing UK organisations. We work closely with the NCSC and last year developed a Ransomware Guide for organisations experiencing a ransomware attack. Our guide aims to minimise the impact of a ransomware incident, particularly on disruptions and costs to businesses, the number of ransoms paid, and size. Since its publication, our guide has been taken up internationally and endorsed by the Counter Ransom Initiative.
44. We submitted a response to the Home Office's consultation on its ransomware proposals earlier this year and have been closely engaging with government officials as those plans develop. We would like to have clarity on how the Bill's incident reporting requirements would be developed alongside the ransomware proposals being progressed by the Home Office, given how cyber security overlaps across several departments.
45. **We have serious concerns regarding the Home Office ransomware proposals.** We're concerned by the potential economic impact of introducing a targeted ban on ransomware payments and the development of a ransomware payment prevention regime covering the whole economy. **These proposals, while well intentioned, could lead to increased costs for businesses, business interruption, and potential insolvencies causing significant economic harm.** This is particularly acute for SMEs, which often lack both operational resilience and cyber insurance cover. Smaller firms simply can't withstand extended downtime, and without insurance or clarity on permissible actions, insolvency becomes a real risk.
46. These impacts can be mitigated by calibrating the details of the ransomware regime carefully. We look forward to continuing engaging with the government to achieve our shared ambitions to develop a ransomware regime that works for UK businesses and strengthens cyber security.