Submission to the Public Bill Committee: Cyber Security and Resilience (Network and Information Systems) Bill

The British Insurance Brokers' Association (BIBA)

Executive summary

BIBA supports the Bill's objective to strengthen the security and resilience of network and information systems by widening the scope of the NIS regime, improving incident reporting, and strengthening enforcement consistency. The Bill's provisions on "critical suppliers" are particularly important given the growing role of supply chains in systemic cyber risk, seen in the series of high-profile UK cyber-attacks in 2025.

However, improving resilience also requires raising preparedness across the wider economy – especially among SMEs – where cyber risk is prevalent, but cyber insurance and the professional advice of brokers remain under-used.

59% of UK businesses experienced a cyber-attack in the last 12 months[1], with many experiencing operational and financial disruption. Yet 35% of SMEs have no cyber insurance[2], and standalone cyber policies have extremely low penetration (2.8%) across UK businesses[3].

Cyber insurance is not just a financial product; it can be a practical cyber resilience tool. Proactive cyber insurance can provide access to incident response, threat monitoring and vulnerability scanning, technical support and recovery services – helping a business stay operational and limiting the kind of wider economic disruption we saw last Summer. Brokers can help firms assess risk and purchase cover that matches their risk profile, helping improve cyber controls especially where knowledge is limited, or does not exist in the case of many SMEs and micro-businesses.

BIBA's recommendations to support the Bill's aims are:

1. **Make cyber insurance a more explicit part of the UK's resilience toolkit** through a national awareness approach and greater Government–industry collaboration.
2. **Support and recognise broker-led capability building**, for example, through accreditation, directories of expert cyber insurance brokers, training, and clearer terminology.
3. **Consider a backstop for extreme systemic cyber events**, for example via a "Cyber Re" scheme (akin to Pool Re).
4. **Properly incentivise SME uptake of cyber insurance**, including, for example, removing Insurance Premium Tax for SME cyber policies.
5. **Keep implementation proportionate and avoid duplicative burdens**, so compliance costs don't crowd out real security investment, particularly for SMEs in supply chains.

The state of UK cyber resilience: persistent attacks and a protection gap

There is a widening gap between the scale of cyber risk and the level of insurance protection in place, particularly for SMEs. The Hiscox Cyber Readiness Report (September 2025) reports that 59% of respondents suffered a cyber incident in the past year, and one third (33%) faced a substantial fine after a data breach affecting financial health.

[1] Hiscox Cyber Readiness Report, September 2025
[2] Department of Science Innovation & Technology
[3] Research by Broker Insights

Despite this, uptake of cyber insurance remains low. DSIT survey evidence shows that 35% of SMEs have no cyber insurance and there is just 2.8% penetration for standalone cyber policies across UK businesses (Broker Insights).

This matters because when incidents occur, impacts are both operational and financial, with 70% of organisations experiencing a "significant" or "very significant" disruption to business because of a breach (IBM's Cost of a Data Breach Report 2024). Cyber insurance, alongside good cyber security hygiene, can be a critical lever for recovery and continuity.

Interconnected supply chains mean cyber incidents can spread economic harm beyond the directly affected organisation. As we have seen, a single attack on a major company can cascade into order cancellation and acute cashflow strain for dependent SMEs. New insurance products such as "customer business interruption" cover – protecting supply chains from cyber-attacks on their key customer businesses – continue to broaden the support that cyber insurance can provide.

BIBA's recommendations to support the Bill

1. Make cyber insurance a pillar of national cyber resilience policy

BIBA calls for the Government to actively collaborate with the insurance industry to raise awareness of cyber resilience and to promote cyber insurance as a key pillar of its cyber resilience strategy as part of a national awareness campaign (with DSIT and the NCSC). This would complement the Bill's objective of strengthening resilience across critical and interconnected sectors.

The Statement of Strategic Priorities provision of the Bill is an opportunity to embed financial resilience and risk management alongside technical cyber controls.

2. Support broker-led capacity building, including accreditation, directories, clearer language, and training

Insurance brokers play a key role in helping firms understand risk, improve controls, and access appropriate cover. The Bill strengthens the use of guidance and strategic priorities to drive consistent cyber resilience outcomes across sectors, including through provisions on coordinated guidance for critical suppliers. Insurance broker-led capability building provides a practical route to implement those priorities across SMEs and supply chains.

BIBA has set out commitments in its 2026 Manifesto to support and engage with DSIT on an accreditation process for expert cyber insurance brokers promoting cyber resilience and to build a BIBA directory to which businesses seeking cyber insurance can be signposted. BIBA also commits to working with market bodies to develop common terminology and "de-mystify" cyber policy language, alongside training and educational resources.

BIBA already runs several directories including for the FCA, HM Treasury, Flood Re and the ABI and we are a not-for-profit organisation. Gov.uk could help signpost to the accredited cyber insurance broker directory to help SME's more easily access suitable cover.

3. Consider a backstop for extreme systemic cyber events (i.e. a "Cyber Re")

While a strong private insurance market is the key for day-to-day protection, a Government-backed pool covering the most extreme events, with very clear triggers, could be a solution where losses are too large for the private market alone. Precedent exists with Pool Re.

This could be explored in parallel with the Bill, particularly given the Bill's attention to systemic dependencies (data centres, managed services, critical suppliers).

4. Incentivise SME uptake, including removing IPT for SME cyber policies

BIBA proposes that the Government encourage uptake by, for example, making cyber policies for SMEs exempt from Insurance Premium Tax. As established, over a third (35%) of SMEs have no cyber cover at all. Our 2025 polling with Opinium additionally showed that 35% of SMEs have had to reduce their insurance cover in the past year to save money. Meanwhile, 62% of UK businesses report that they would increase their insurance cover if they were financially able to.

This presents an opportunity to use financial incentives to close the cyber protection gap and build economic resilience across businesses and supply chains

5. Keep implementation proportionate, and avoid duplicative burdens

BIBA recognises the importance of effective enforcement. The Bill includes enhanced powers around cost recovery and charging schemes. While these tools can support consistent regulation, the regime must remain proportionate – especially where SMEs may be indirectly affected as suppliers or service providers – so that compliance costs do not crowd out investment in real security improvement.

Conclusion

BIBA supports the Bill's intent to modernise the UK's cyber resilience framework by expanding coverage to key parts of the digital ecosystem, strengthening incident reporting, and enabling clearer strategic direction. To maximise the Bill's impact, it should be used as a platform to close the cyber protection gap, particularly among SMEs, by promoting cyber insurance as a core component of resilience, incentivising uptake (including IPT relief), supporting insurance broker-led advice and capability building, and considering options to address truly systemic "catastrophic" cyber incident scenarios. We stand ready to offer practical support with the creation of a cyber insurance broker directory.

About the British Insurance Brokers' Association

The British Insurance Brokers' Association (BIBA) is the UK's leading general insurance intermediary organisation representing the interests of insurance brokers, intermediaries, and their customers.

BIBA membership includes around 1800 regulated firms, employing more than 100,000 people. General insurance brokers contribute £26.1bn to the UK economy and arrange 77% of all general insurance and 94% of all commercial insurance, with a total estimated premium of £150bn. Insurance brokers put their customers' interests first, providing advice, access to suitable insurance protection and risk management.

BIBA helps more than 430,000 people a year to access insurance protection through its *Find Insurance* service.