Zurich UK response to Cyber Security and Resilience (Network and Information Systems) Bill: call for evidence

About us

Zurich UK (Zurich) provides a suite of general insurance and life insurance products to retail and corporate customers. We supply personal, commercial, and local authority insurance through a number of distribution channels, and offer a range of protection, retirement, and savings policies available online and through financial intermediaries for the retail market and via employee benefit consultants for the corporate market. We have several large office sites regionally and employ around 5,000 people.

We are part of Zurich Insurance Group, a leading multi-line insurer serving people and businesses in more than 200 countries and territories. Founded over 150 years ago, the Group provides insurance protection and prevention services that promote wellbeing and enhance climate resilience. The Group has about 60,000 employees, is headquartered in Switzerland and Zurich Insurance Group Ltd (ZURN) is listed on the SIX Swiss Exchange.

Zurich provides cyber insurance to larger companies and through Zurich Resilience Solutions (ZRS), it's risk consulting arm, supports customers in the public and private sector to enhance their cyber resilience capabilities.

Zurich welcomes the introduction of the Cyber Resilience & Security Bill into Parliament. Insurance plays a multifaceted role in enhancing cyber risk management and resilience. It provides financial protection, supports incident response and recovery, encourages the adoption of best practices, and offers valuable insights into cyber risk trends.

Response

Zurich supports the Association of British Insurer's (ABI) response to this call for evidence noting the following:

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.

3. 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.

4. 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.

5. 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).

6. 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.

7. 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.

8. 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

9. 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.

10. Clearly delineate the responsibilities of businesses, insurance, and government in cyber security and understand where the industry can and cannot support these goals.

11. Work with our sector to raise awareness of the value of cyber insurance and address the cyber resilience of SMEs.

12. 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.

13. Clear and timely guidance for firms under the Bill's scope to help with compliance.

14. 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.

15. 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.