Labour International Advisory:

Cyber Security and Resilience (Network and Information Systems) Bill

Resilient services, responsibly built

Labour International supports the Bill, and asks Parliament to extend its protection to retail and communications, and to make it work for small firms, the environment and democratic accountability.

204
nationally significant cyber incidents handled by the NCSC, year to Sept 2025 (89 the year before)

£14.7bn
cost of significant cyber attacks on UK businesses in 2024, about 0.5% of GDP

863
newly regulated firms: 788 managed IT providers, 64 data centres, 11 load controllers

The Bill in 30 seconds

- **What it does.** Extends the 2018 NIS Regulations to managed IT providers, data centres (from 1 MW) and large load controllers (300 MW+), adds critical suppliers, and requires a first incident report within 24 hours.
- **Why now.** Attacks on Marks and Spencer, Jaguar Land Rover and NHS supplier Synnovis (11,000+ delayed appointments) show how suppliers and firms outside today's regime can bring services down.
- **The catch.** It is a framework. Security duties, new sectors, fines of up to £17m or 10% of turnover and national-security directions follow in regulations, so commitments made now matter.

Five asks of Labour Members

1. Protect small firms and the people who keep services running. Back a free SME advice and incident-response service using existing NCSC routes, and scale reporting duties to size.

2. Extend responsibilities to the sectors the public depends on most, and align the regimes. Retail is outside the Bill, despite the 2025 Marks and Spencer attack. Public telecoms already have security duties, codes and fines of up to 10% of turnover under the Communications Act 2003, so the aim is alignment, not duplication: ask for a gap analysis and add any power the Bill gives other sectors that the Act lacks (such as customer warnings or critical-supplier designation). Duties should be proportionate to the risk to the public, not firm size. We support the Camrose and Markham amendment for a published assessment, within 12 months, of further strategically important entities.

3. Verify resilience, do not just document it. Resilience should be proven by objective testing, not paperwork alone. The EU's Digital Operational Resilience Act (DORA) requires designated financial entities to undergo threat-led penetration testing of live critical systems at least every three years, by qualified testers under regulator supervision, with defenders not told. Ask the minister to commit that regulations and the code of practice will provide similar independent, unannounced testing for the highest-risk operators, with safety first (agreed limits, kill switches, engineering sign-off for control systems) and accredited testers independent of the firm and its suppliers.

4. Make resilience green. The government's impact assessment finds "no direct environmental impact". We disagree: load control underpins Clean Power 2030, and data centres are energy- and water-intensive. Seek commitments that regulators and the code of practice (a) have regard to sustainability, always subject to security; (b) favour low-carbon backup power, efficient cooling and heat reuse; (c) share energy and water data already held; and (d) publish an environmental assessment before major regulations.

5. Keep power accountable. Press for a first review of the regime within three years rather than five, annual public reporting on incident numbers and on national-security directions in aggregate, and a clear route to protect good-faith security researchers.

Our view on the amendments tabled for Report

SUPPORT	Final incident report within 14 days and prompt customer warnings, and voluntary near-miss reporting (Harding, Kidron, Clement-Jones); annual incident-volume report; UK-EU NIS2 divergence report; free SME advice and incident service (Northover); regulate by risk, not firm size (Morgan of Cotes); 12-month assessment of further strategically important entities, and annual reporting by large regulated businesses on their cyber plans (Camrose, Markham); review of a Computer Misuse Act defence (Clement-Jones).	Cheap, evidence-building and proportionate; the strategic-entities assessment is the evidence route for adding retail and other sectors. Keep reports scaled for small firms.
PROBE	Narrowing the "managed service" definition (Clement-Jones); incident reporting by frontier AI developers (Harding, Kidron, Clement-Jones); Digital Sovereignty Strategy (Kidron, Clement-Jones); consultation on ransomware amnesty reporting, consultation on data minimisation, and a review of information sharing and analysis centres (Camrose, Markham).	Worthwhile ideas needing changes or commitments: a ransomware safe harbour must not excuse poor protection; one month is too short for the data consultation; review the centres, not their enforcement powers.
DO NOT SUPPORT	Delaying commencement until the National Cyber Action Plan is published (Camrose, Markham, cl. 60); AI Security Institute pre-deployment audit (Tarassenko) and standards and enforcement powers (Clement-Jones); statutory AI "red lines" (Kidron, Clement-Jones); "last-resort" shutdown of data centres and large AI systems (Clement-Jones); professional title required of every responsible individual (Northover).	Would delay overdue protection, put sweeping AI regulation into a cyber-resilience Bill, or cause the outages they aim to prevent. Publish the Action Plan elements without making them a gate; cover frontier AI in AI legislation.

Our guiding principles

- **Resilience comes first.** Services the public relies on must keep running; where aims conflict, security wins.
- **Verified, not performative.** Resilience is proven by independent testing of real systems, not by paperwork alone.
- **Proportionate and risk-based.** Duties follow the harm a failure could cause, not the size of the firm.
- **Support, not just enforcement.** Smaller firms and regulators need help to comply.
- **Environmental responsibility is part of resilience.** Digital infrastructure should not lock in avoidable energy, water and waste costs.
- **Accountable power.** Wide powers need transparency, review and protection for good-faith researchers.
- **Aligned with partners.** Alignment with EU NIS2 cuts duplication for firms operating in both.

Where to find more

- **Full briefing and position papers:** available on request (see contact below).
- **The Bill and amendments:** bills.parliament.uk/bills/4035 (HL Bill 49 running list, to 13 October 2026).
- **Impact assessment:** DSIT final stage assessment (updated 13 May 2026); Lords Library briefing HL Bill 32 (updated 23 July 2026); Lords Committee stage summary.

Talk to us

Labour International members work in cyber security, data-centre operations, energy and EU compliance, and can brief you or your staff on how the Bill works for firms operating across the UK and EU.

Contact: LI Briefings | briefings@labourinternational.net

Sources: NCSC, KPMG and DSIT impact assessment figures as cited in the Lords Library briefing; positions based on the amendment list to 13 October 2026. Report date provisional; environmental points are our own assessment.