AUGUST 2025

CURATED

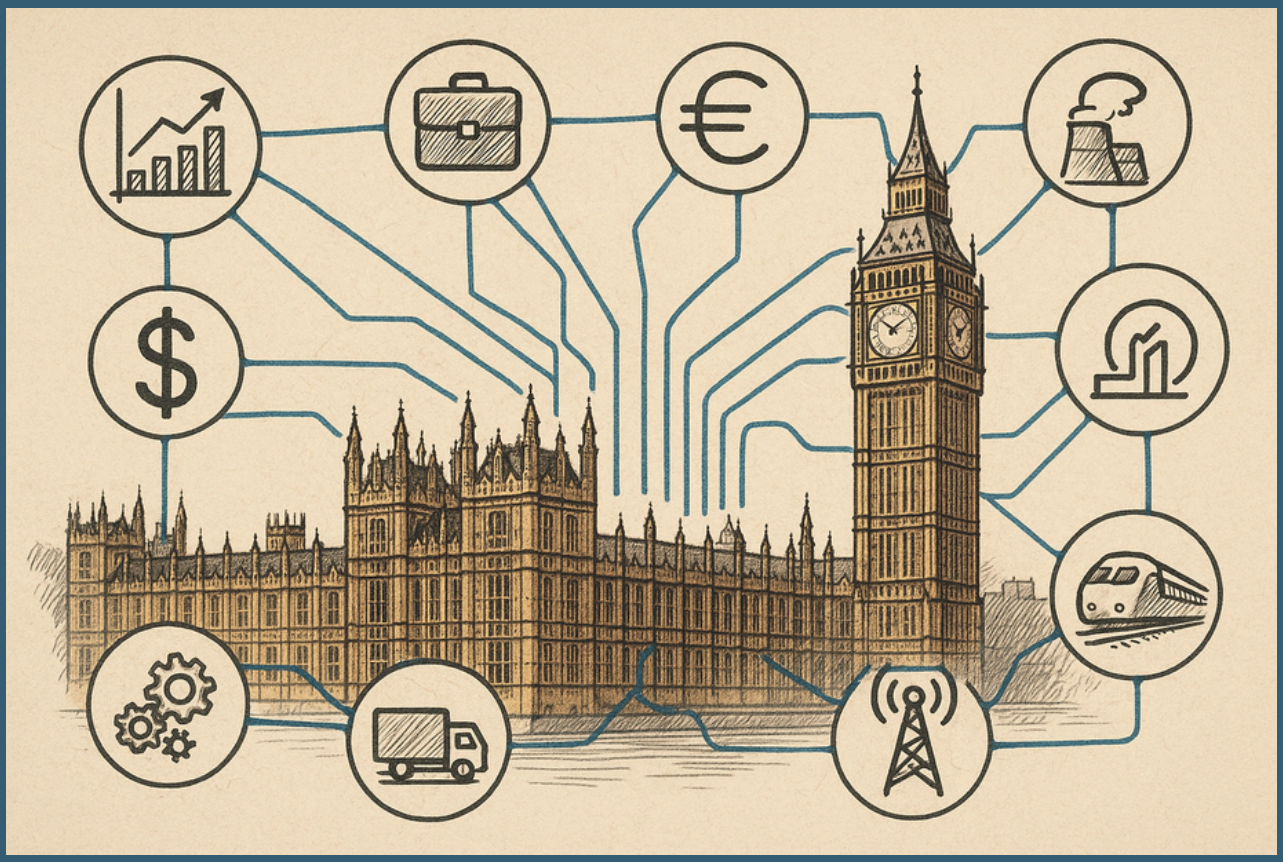
SO WHAT?

THE CYBER SECURITY AND RESILIENCE BILL (2025)

READ ON

INTRODUCTION

The UK government has introduced the Cyber Security and Resilience Bill (CSRB) in 2025 to strengthen digital resilience across all sectors, especially businesses and those that supply critical national infrastructure. Although the main headlines focus on large providers, the Bill directly impacts smaller companies, particularly those in supply chains or providing digital/IT services to essential sectors. Is it important to you? Is it close to anything already in place? Why does it matter?



Why This Bill Matters to SMEs

- **Scope Expansion:** The Bill brings more businesses; including managed service providers (MSPs), IT companies, and data centers, all into the scope of cyber regulation. Even if you're not running the NHS or a water utility, if you serve these sectors, you could be within the scope

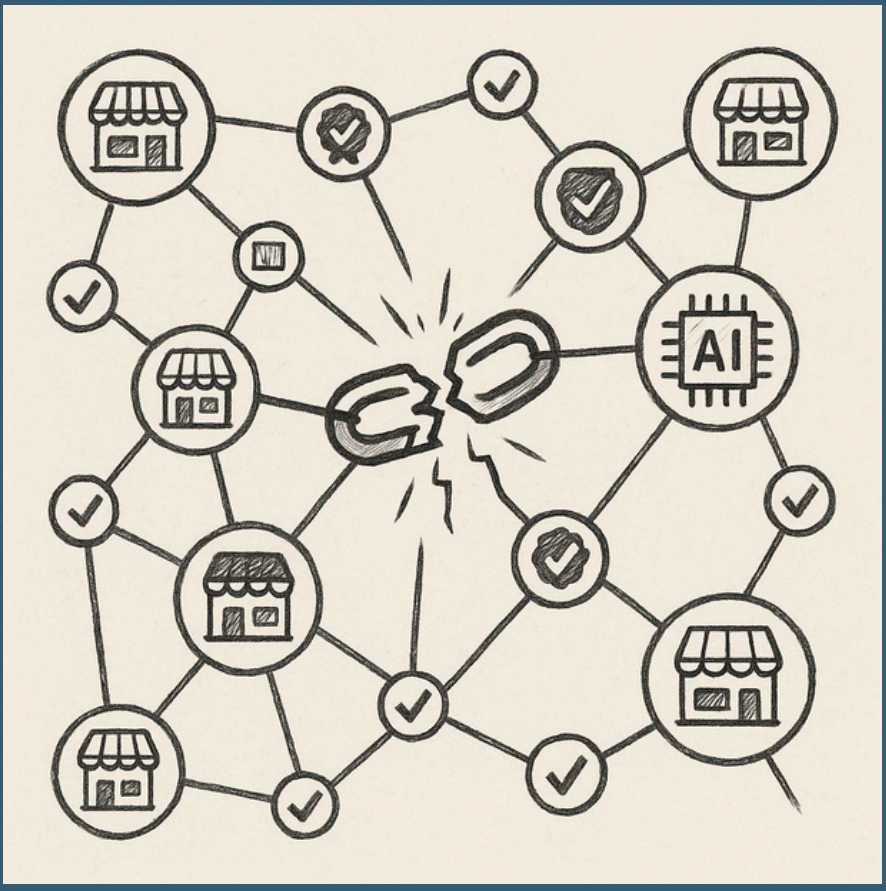
- **Tougher Standards:** There's an increased focus on proactive risk management, evidence-based cyber strategy, and supply chain resilience.

- **Incident Reporting:** You'll need to rapidly report cyber incidents, not just breaches, but also events that *could* affect essential service delivery.

- **Stronger Regulator Powers:** Regulators have enhanced inspection and enforcement powers (including substantial fines for non-compliance).

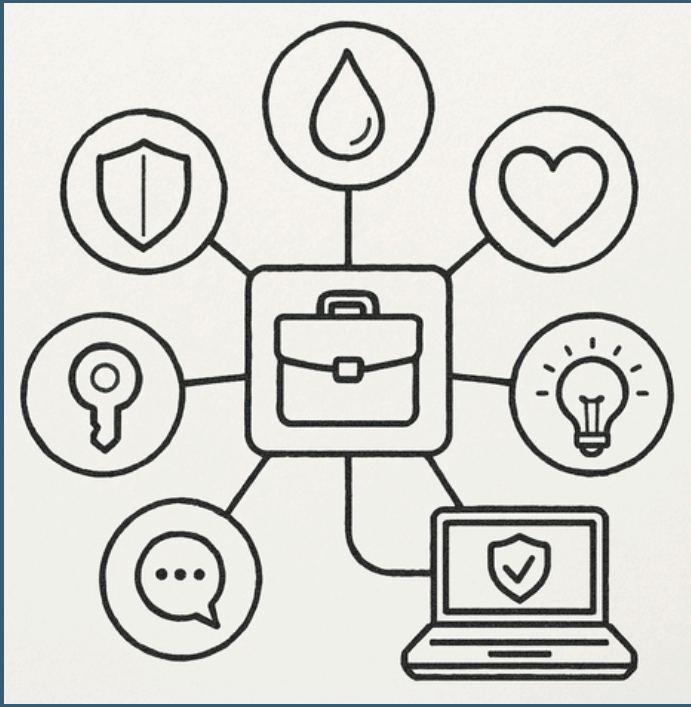
What's Changing from the Existing NIS Regulations?

- **Wider Coverage:** The NIS Regulations (since 2018) applied to Operators of Essential Services (OES) and certain digital providers. The new Bill adds more suppliers (including many SMEs) to this list.
- **Supply Chain Focus:** Recognises that attacks on one supplier can disrupt the whole system; you're expected to manage and evidence third-party cyber risks.



- **Adaptability:** The government can quickly adapt rules as cyber and technological threats evolve mainly due to the increasing threats from AI-powered attacks which continue to rise.
- **Certification Emphasis:** Expect more emphasis on government-backed cyber certifications (e.g. Cyber Essentials, IASME Cyber Assurance) as proof of compliance, trusted by insurers and customers alike.

What Should Business Owners and Directors Do Now?



1. Review Your Place in the Supply Chain

Check whether your services/products support “essential” sectors (health, energy, water, transport, digital infrastructure).
Assess if you’re handling sensitive data, supporting critical operations, or are a key service provider.

2. Assess and Upgrade Your Cyber Hygiene

Obtain or renew a certification such as Cyber Essentials or IASME Cyber Assurance. This shows you meet some level of minimum security standards that are favoured by some agencies.

Make sure passwords and remote access follow current best practices (look into passwordless authentication where possible as this is part of the new framework).

3. Strengthen Internal Policies and Training

Update and test incident response, access control, data protection, and business continuity plans.
Regular staff training: Phishing simulations and awareness sessions can prevent substantial user-related incidents. With some estimates as high as 90%.

4. Supply Chain and Partner Vigilance

Ask suppliers and partners for proof of their cyber defences, especially if you depend on them for operations or IT.
Record what checks you make, evidence will be critical if there’s a cyber incident.

5. Continuous Monitoring and Resilience

Use pen testing and vulnerability scans to fix weak points in your networks.
Consider continuous security monitoring, either in-house, via an IT consultant.
Better done more than once per year.

6. Incident Reporting Readiness

Ensure clarity on how and who will report cyber incidents to regulators, don't wait until you're in crisis mode.
Document and periodically rehearse your incident response process.

7. Potential Cost and Efficiency Impacts

Budget Impact: You may need to allocate more budget for IT security, certifications, staff training, and possibly specialist consulting. At present we see 1% - 1.5% of turnover spent on cyber security alone as a starting point.
Time Investment: Expect to dedicate time to compliance tasks, keeping documentation up-to-date, conducting checks, and managing supply chain due diligence.

Action Points: What to Start Doing Now

- Review who in your business is responsible for cyber security and, if necessary, assign clear roles, even without a dedicated IT team.
- Contact current IT or MSP partners to schedule risk assessments and compliance certifications.
- Begin updating staff policies to include scheduled cyber awareness training.
- Start gathering and documenting supplier cyber credentials.
- Prepare a simple response plan, including "who calls the regulator" in a cyber incident.

Bottom Line:

The new Bill will make cyber resilience an ongoing, routine part of your business operations, not a one-time project or annual task. While it might feel like extra red tape, these routines actually safeguard your profits, reputation, and contracts. Embracing a "little and often" approach to security best practices will help avoid fines, reputational harm, and disruptive incidents, protecting your business in the long run.

What specific actions can my small business take now to prepare for upcoming regulations

Here are practical steps your business can take right now to prepare for the upcoming Cyber Security and Resilience Bill (2025). These actions can help ensure both compliance and real protection against cyber risks, even if you don't have a dedicated in-house cyber team.

1. Map Your Regulatory Exposure

- Check if you supply or support essential sectors (health, transport, energy, water, digital infrastructure).
  - List all clients operating in regulated sectors.
  - Identify any "critical" data, system, or service you provide.
- Action: Create a simple list to document which contracts or clients connect you to regulated sectors.

2. Upgrade and Certify Your Cyber Hygiene

- Certification: Pursue or renew recognised certifications like Cyber Essentials or IASME Cyber Assurance.
- Passwords & Access: Implement multi-factor authentication (MFA) on all accounts; use password managers or consider passwordless access.
- Patch Management: Ensure all software and devices are set for automatic security updates.
- Action: Assign a staff member or IT partner responsibility for ongoing certification and update policies.

3. Train Staff Regularly

- Basic Awareness: Schedule quarterly cyber awareness sessions, focus on phishing, safe data handling, and incident response.
- Simulation Drills: Run simple "phishing test" emails or pose "what would you do if…" cyber scenarios.
- Record Keeping: Maintain an easy log of who's attended training.
- Action: Use low-cost online platforms or ask your IT provider for training options.

4. Strengthen and Document Internal Policies

- Incident Response: Update or draft a basic incident response plan (clear “who does what, when”). Practice with a tabletop exercise.
- Access Controls: Review who has access to key systems, remove ex-employees, avoid sharing logins.
- Business Continuity: Ensure you have simple data backup procedures; test restoring from backup at least annually.
- Action: Keep these documents short and accessible; save templates for easy updates.

5. Vet Your Suppliers and Partners

- Supplier Checks: Ask suppliers (IT support, MSPs, software vendors) for proof of their own cyber certification.
- Update Contracts: Add clauses requiring suppliers to maintain cyber defences and inform you of incidents.
- Record Due Diligence: Keep screen grabs or copies of certificates in your records.
- Action: Build a simple “supplier checklist” you update each year.

6. Improve Continuous Monitoring

- Vulnerability Assessments: Schedule at least annual pen tests and regular vulnerability scans. Although we recommend more frequently than annually.
- Ongoing Monitoring: If possible, adopt a basic monitoring tool (or ask your IT partner) to watch for unusual activity or intrusions.
- Action: Document when checks happen and what was found/fixed.

7. Plan for Incident Reporting

- Reporting Plan: Identify one person responsible for regulator notifications if a cyber incident occurs.
- Templates: Draft, in advance, the kind of incident log or template you'll need to fill in.
- Practice: Do a "dry run" so everyone knows the process.
- Action: Make this a standard part of your business continuity planning.

8. Budget and Assign Responsibility

- Budget: Allocate funds for training, certification, and IT security upgrades now, don't leave it to year-end surprises. Typically businesses assign between 1% - 1.5% of turnover on cyber security alone.
- Roles: Even in a small business, assign who handles cyber tasks; don't assume "someone else" will.
- Action: Review progress monthly in management meetings.

Why Start Now?

Preparing before regulations come in force shows your business is proactive, which helps avoid fines, ensures eligibility for contracts, and reduces risk of costly cyber attacks. Taking these steps doesn't require heavy technical know-how, just practical management, planning, and using the right support when needed.

AUGUST 2025

CURATED

WANT TO HAVE A SAY ?

ASK A QUESTION OR GET IN TOUCH
ENQUIRIES@INCOMMSEC.COM