



**THE
UK CYBER SECURITY AND RESILIENCE
(NETWORK AND INFORMATION SYSTEMS)
BILL (CSRB) IS HERE!**

**IT'S MANDATORY. READ ON TO FIND OUT
WHAT YOU NEED TO KNOW.**



MicroSystem Support

“[In 2024], the UK was the most targeted country in Europe for cyber attacks, and looking across all cyber incidents, over 40% of UK businesses experienced cyber-attacks – equivalent to over 600,000 organisations.

Cyber attacks are estimated to cost UK businesses £14.7 billion each year, equivalent to 0.5% of UK GDP.”

UK Department for Science, Innovation & Technology,
Policy paper, Summary of the Bill, 12 November 2025

12th November 2025: The UK Cyber Security and Resilience (Network Information Systems) Bill (CSRB) has been introduced to Parliament.

It reforms the UK Network Information Systems (NIS) regulations 2018.

CSRB has expanded its scope and broadened government powers to enable much-needed cybersecurity and business resilience measures that impact all of us in the UK.

The regulations require organisations to manage risks if they relate to the functioning of network and information systems that are relied on, specifically:

Cyber Security Risks - Protection against threats such as hacking, malware, ransomware, and data breaches.

Physical security and broader operational resilience risks - Protection against disruption arising from physical threats and hazards.

If you are in any of the following business or service sectors and trade within the UK, then it applies to you.

It is mandatory.

Operators of Essential Services (OES) that were originally in scope remain as:

- **Energy:** Electricity, oil, and gas.
- **Transport:** Air, rail, water, and road.
- **Health:** Healthcare settings (including hospitals, private clinics, and online settings).
- **Water:** Drinking water supply and distribution.
- **Digital infrastructure:** TLD (top-level domain) name registries, DNS (domain name systems) service providers, and IXP (Internet exchange point) operators.

Thresholds for each sector are specific to several factors such as their services, the size of the customer base, the impact on customers, and geography (Great Britain and Northern Ireland).

Relevant Digital Service Providers (RDSPs)

that were in the original scope also remain:

- **Online search engines:** “online search engine” means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found.”
- **Online marketplaces:** “...a digital service that allows consumers and/or traders... to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace.”
- **Cloud computing services:** “...a digital service that enables access to a scalable and elastic pool of shareable computing resources.”

Additional sectors and services that are now in scope:

- **Data centres:** For example, those that hold patient records, emails, and financial data.
- **Managed service providers:** Outsourced IT services that are essential to OESs and RDSPs.
- **Large load controllers:** Organisations managing electrical loads for smart appliances, e.g., to support electric vehicle (EV) charging during peak times.
- **Designated critical suppliers:** Regulators will be able to designate critical suppliers, ensuring the most important suppliers to essential and digital services are subject to the regulatory regime.

Exemptions

Micro and small enterprises are exempt. The Bill points to the EU NIS for reference to these:

- **Enterprises:** Employ fewer than 250 persons, annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.
- **SMEs:** Small enterprises employing fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.
- **Micro-enterprises:** Employing fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.

12 sector-specific regulators are responsible for implementing these laws.

The Bill provides them with expanded powers:

Incident Reporting and Increased Scope

“More forms of harmful cyber breaches will need to be reported to regulators, where they have the potential to cause significant impacts, with initial notification within 24 hours and a fuller report within 72 hours.”

Increased Fines

- Up to £17 million, or 4% of a regulated entity's worldwide turnover, whichever is higher for more serious breaches,
- Up to £10 million, or 2% of a regulated entity's worldwide turnover, whichever is higher, for less serious breaches.

Powers of Direction - Focused Scrutiny

“The government will be able to direct regulators or regulated entities to take targeted and proportionate action in response to imminent threats that risk UK national security.”

The Bill is in response to the daily threats to our society, businesses, and lives.

Microsystem Support is here to help you be safe and compliant.

From December 2025, our ***SME Insights*** webinar series will cover CSRB and how to be compliant and safe.

Contact us to learn more.



MicroSystem Support

www.microsystem.co.uk

info@microsystem.co.uk

01179 599 393

Cyber Security
IT Infrastructure
HPE AI Hardware and
Software Toolset
Consultancy
Hardware
Software
Support

