# UK Cyber Security and Resilience Bill

(see https://bills.parliament.uk/bills/4035)
(See Government Cyber Action Plan).

**Roundtable**

**9th March 2026**


## Gill Ringland

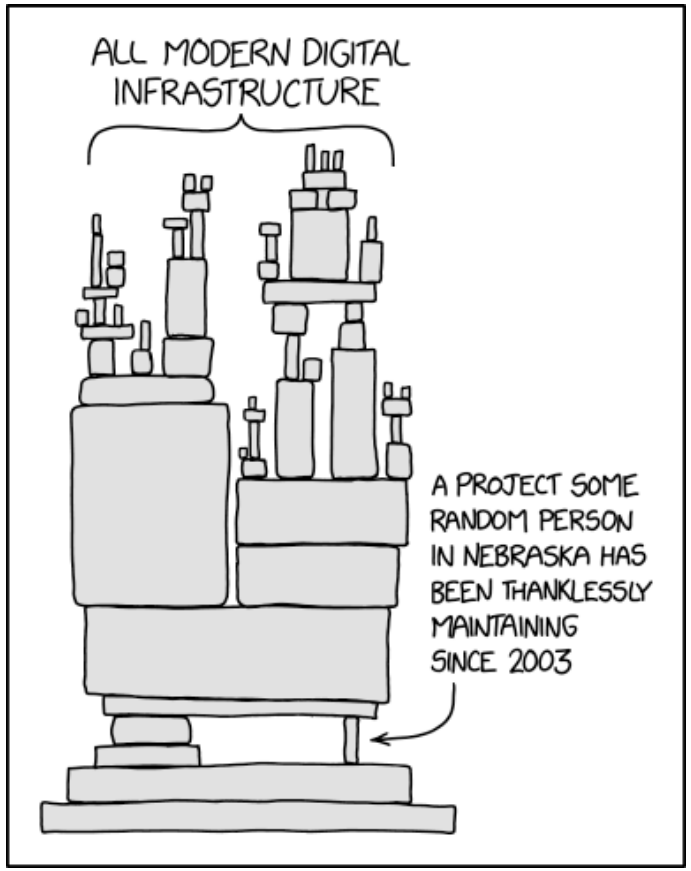
**Co-chair, BCS ITLF Availability and Service Resilience Working Group**


# What is cyber security and resilience?

- Cyber security and resilience mean defending information technology (IT) systems from, and mitigating the impact of, attempts to gain unauthorised access to or control of those systems (cyber attacks).
- With the UK economy and society increasingly dependent on digital processes supplying online services, the potential impact of successful cyber attacks is significant.
- The CEOs of the FTSE350 companies have been urged by the UK Government to look toward "resilience engineering", systems that can anticipate, absorb, recover, and adapt, in the event of IT threats.
- In UK Government Departments, the Accounting Officer is the senior official (Permanent Secretary or CEO) with overall accountability for an organisation. This includes personal accountability for the cyber risk of that organisation.
- IT threats to digital services are not only cyber, eg cutting of cables, meltdown of power supply, software failures, disinformation.

# Digital services are delivered through tightly coupled complex software systems

- Cyber attacks are not the only cause of failure
- Tightly coupled complex software systems are liable to unpredictable failures
- More lines of code, variable quality from many sources – COTS, open source
- Global software supply chains
- Pressure for new features limits ability to build in architectural resilience features
- Natural Accident Theory applies



# Service resilience – some definitions

- Risk - *expose (someone or something valued) to danger, harm, or loss*
- Service – *the action of doing work on behalf of another*
- Service resilience - *action to prevent or mitigate risk to services*
- Operational resilience – *an organisation's ability to respond to and overcome adverse circumstances during operations that might cause outages or malfunctions with financial loss or disruption of services to users*
- Digital service resilience – *resilience that comes from the ability of the digital systems to prevent or mitigate IT risk as measured on user side as in NIS Framework.*
- NIS Framework - *measures Availability to users: Lost user hours; Damage to users' data; Damage to users' life or health; Users' financial loss.*

# Scope of the Bill – NIS Regulation

## NIS regulation applies to two groups of organisations:

- operators of essential services' (OES): this includes CNI - critical infrastructure (water, transport, energy) and also other important services, such as healthcare and digital infrastructure;
- relevant digital service providers' (RDSPs).

## The bill would expand the scope of the NIS Regulation to include:

- data centres (which "host and support the digital infrastructure that underpins modern life");
- large load controllers (organisations that can control the energy use of smart appliances such as batteries and electric vehicles);
- managed service providers (organisations that provide third-party IT services to other businesses);
- suppliers that are critical to a regulated organisation's ability to provide its essential service.

# Scope of the Bill – enforcement of regulations

**Enhance regulators' ability to implement and enforce the NIS Regulations consistently across sectors by:**

- **requiring regulated organisations to report more cyber incidents enabling regulators to recover costs, share information, and impose higher fines.**

**Empowering the Secretary of State to:**

- **publish a statement of strategic priorities setting out objectives for regulators to achieve when carrying out their functions under the NIS Regulations.**
- **direct regulated organisations and regulators to take specified actions in the interests of national security.**
- **update the NIS Regulations through secondary legislation rather than primary.**

# Some topics for discussion

- What non CNI organisations can learn from the Bill's direction of travel.
- How to balance cyber security with wider business resilience objectives.
- Whether the Bill will encourage a deeper consideration of customer effects and company liability.
- The current landscape of governance frameworks, standards, guidance, and regulation – and where gaps remain.
- The role of IT, security, risk, business continuity, audit, and assurance professionals in building resilience and trust.
- Whether existing skills are sufficient to achieve operational resilience.
- What information IT and security teams need to provide to support effective oversight.

# Roundtable discussion

**Roundtable**

**9th March 2026**

**At your table:**

- **Choose a topic from the list**
- **Appoint a rapporteur**
- **Be ready to feedback at 18:50, max  2 minutes and 3 points**

**Then we have a plenary discussion**

ISACA

IT Leaders Forum

# Thank you!

**Roundtable**

**9th March 2026**


Sue Milton – ISACA --- sue.milton@ssmga.uk

Gill Ringland – BCS --- gillringland@gmail.com

Ed Steinmueller – BCS --- w.e.steinmueller@sussex.ac.uk


And now, please join us for refreshments ----