An introduction to the upcoming UK Cyber Security and Resilience Bill and the EU Network Information Security Directive (NIS2)

On 9 April 2025, the UK government published details of the Cyber Security and Resilience Bill (CSRB), a mandatory requirement that is to be formalised later this year. This is a major step forward in addressing cyber threats to the UK's Critical National Infrastructure (CNI) which have a significant impact on public welfare and national security.

This announcement detailed the government's intention to expand on the UK's current Network and Information Security regulations and to learn from the European Union's much expanded Network and Information Security Directive (NIS2).

Whilst the CSRB is not finalised, businesses that trade in the UK (and in certain cases with the UK) can prepare for compliance now by gaining a working knowledge of NIS2 regulations to understand their impact on Information Technology (IT), Operational Technology (OT), and services within the scope of requirements.

The operational and infrastructure impacts on businesses are far reaching, and, from an IT infrastructure services provider's perspective, there are many ways that MicroSystem Support Ltd can support organisations to be compliant with NIS2 and to prepare for CSRB.

Threats from cyberattacks to national infrastructures and the public continue to escalate as nations face relentless waves of attacks, continuously evolving in sophistication and effectiveness.

According to the Thales Data Threat Report 2024, 93% of CNI organisations saw a rise in cyberattacks, with 42% suffering a data breach.

The UK government's Cyber Security Breaches Survey 2024 found that in the UK alone 70% of medium-sized businesses and 74% of large businesses reported a cybersecurity breach or attack between 2023 and 2024.

This blog post is an abridged version of the full white paper that can be found here.

The EU Network and Information Security Directive (NIS2)

NIS2 addresses the impact of cyber threats on organisations that are important to a country's infrastructure and facilitates cross-border collaboration across EU Member States. It came into effect across the EU on 16 January 2023, and Member States were required to transpose NIS2 into their national laws by 17th October 2024.

Which Organisations and Sectors Are In Scope?

The Directive focuses on sectors that are crucially important to society and the infrastructure of a nation. These sectors operating in the EU are categorised as either essential or important entities and meet certain financial and organisation size criteria.

Essential entities: 50+ employees, €10 million and above annual turnover or a balance sheet of €10 million or above.

Important entities: 250+ employees, with a €50 million and above annual turnover or a balance sheet of €43 million and above.

Smaller organisations are impacted too. The supply chain section of this blog and the full white paper touches on that topic further.

The Three Pillars of NIS2

ENISA, the European Union Agency for Cybersecurity, breaks down the basis of the Directive into three basic pillars:

1. **National capabilities** that include a cybersecurity strategy, a National Competent Authority (NCA), a Cybersecurity Incident Response Team (CSIRT), a coordinated vulnerability disclosure policy, and the implementation of a cyber crisis management framework.

2. **Cooperation at Union level** through the NIS Cooperation Group, CSIRTs Network, the EU-CyCLONe (European Cyber Crisis Liaison Organisation Network), an EU Vulnerability database, an EU registry for entities, and a published report on the state of the Union with regard to cybersecurity.

3. **Obligations for entities** that include cybersecurity risk management measures, incident reporting, and the responsibility of management bodies.

Compliance is mandatory and leads to enforcement measures followed by heavy fines for non-compliance.

NIS2 Compliance Requirements

The four core elements of the Directive are governance, cybersecurity risk management, reporting, and the use of certified European cybersecurity schemes.

1. **Governance**
   Management bodies of essential and important entities are liable for governance, implementation, and training of cybersecurity risk-management measures, so final responsibility does not fall on the shoulders of IT departments.

2. **Cybersecurity Risk-Management Measures**

   NIS2 outlines the minimum requirements for compliance, taking an 'all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents'. There are ten minimum cybersecurity risk-management measures which are highlighted below and in the white paper, along with ways that MicroSystem Support Ltd can help you achieve compliance.

3. Incident Reporting

Incident reporting is a core element of NIS2. An incident is defined as an event that 'compromises availability, authenticity, integrity, or confidentiality that impacts

stored, transmitted, or processed data, or impacts services via network and information systems.'

In the event of an incident, entities must follow a three-step reporting procedure. An early warning must be issued to the relevant authority within 24 hours, an incident notification within 72 hours, and a final response within one month.

4. **European Cybersecurity Certification Schemes**

   EU Member States encourage essential and important entities to use qualified trust services.

   The ISO/IEC 27000 series is mentioned as an example, with ISO 27001 facilitating compliance by adopting "appropriate and proportionate" technical and organisational measures, and ISO 22301 being 'recommended for business continuity management, assisting in implementing, maintaining, and continuously improving business continuity practices.'

Supply Chain Security

The Directive clearly states the importance of security risk assessments of critical supply chains, taking into account 'both technical and, where relevant, non-technical factors.'

This broadens the impact of NIS2 significantly since supply chain partners of a critical nature can be small or micro businesses.

What Happens If You Do Not Comply with NIS2?

Essential entities face fines of 'a maximum of at least €10,000,000 or of a maximum of at least 2% of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.' (Article 34(4))

Important entities face fines of 'a maximum of at least €7,000,000 or of a maximum of at least 1.4% of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher.' (Article 34(5))

The supervisory and enforcement measures include:

- Ordering entities to make the violations public
- Temporary suspension of services for essential entities that do not carry out remediation
- Personal liability:
    - Publicly naming responsible persons for violations
    - Temporary banning of responsible individuals within essential entities from holding managerial positions

The UK Cyber Security and Resilience Bill (CSRB)

Aligning with the NIS2 Directive and adding further UK-specific requirements, the UK government's CSRB policy statement provides details of measures we should expect to see.

Bringing More Entities into Scope

The UK Government recognises that an increasing reliance on third-party services introduces dangerous vulnerabilities.

The CSRB aims to address this risk by expanding the scope of regulatory compliance and introducing a framework that brings more entities into scope.

Managed Service Providers (MSPs)

MSPs have been specifically named as playing a critical role in the resilience of IT systems, networks, infrastructure, and data.

A managed service is defined as one that:

- Is provided to another organisation (i.e., not in-house), and;
- relies on the use of network and information systems to deliver the service, and;
- relates to ongoing management support, active administration and/or monitoring of IT systems, IT infrastructure, applications, and/or IT networks, including for the purpose of activities relating to cybersecurity, and;
- involves a network connection and/or access to the customer's network and information systems.

Strengthening Supply Chain Security

Supply chain disruption can have a significant and far-reaching impact upon the delivery of essential services. Despite this, there are no targeted mechanisms currently in place to address such vulnerabilities.

The new Bill sets out to tackle this. Regulators will designate high-impact suppliers as 'designated critical suppliers' (DCS), including certain small and micro RDSPs, depending on how critical a role they play in supporting essential services.

This is a significant change as small and micro RDSPs are exempt from the existing UK NIS Regulations.

Bringing Data Centres into Scope

As data centres house and support the technology and data that make them key targets to cyberattackers, they were designated CNI assets in September 2024, and the policy

statement indicates the government's intention to bring data centres into scope of the new regulatory framework.

Other Measures

Other measures that are detailed in the announcement relate to the framework, mechanisms, and processes that the government intends to put in place.

Conclusion

The measures contained in the new Bill are intended to protect our security and vital services. Our nation's infrastructure, its businesses, and each and every one of us as private individuals are targets for cyber attacks every single day. These attacks are relentless, ever-changing, increasingly effective, and they have the potential to create immense harm—to bring vital services to a halt and to compromise the nation's ability to defend itself against hostile states.

The UK CSRB is urgently needed to help us all defend against these attacks.

About MicroSystem Support (MSS)

Businesses ask us how we can assist them in becoming more secure, resilient, and compliant.

Based on the minimum requirements for NIS2, and subsequently the UK CSRB, MSS can help businesses with the ten minimum cybersecurity risk-management measures:

- Policies on risk analysis and information system security
- Incident handling
- Business continuity
- Supply chain security
- Security in network and information systems acquisition, development, and maintenance
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- Basic cyber hygiene practices and cybersecurity training
- Policies and procedures regarding the use of cryptography and, where appropriate, encryption
- Human resources security, access control, and asset management
- Multi-factor authentication (MFA) or continuous authentication solutions, secured voice, video, text communications, and secured emergency communication systems within the entity

We are a specialist SME backed by decades of IT experience. Our ability to be highly reactive, agile to your requirements, and competitively priced makes us the ideal choice to partner with your business.

To learn more how we can help you be ready for CSRB or compliant with NIS2, contact us, or read the full white paper here.