THE UK CYBER SECURITY AND RESILIENCE BILL (CSRB) AND EU NETWORK AND INFORMATION SECURITY DIRECTIVE (NIS2)

EFFECTIVE AND ENDURING PROTECTION IN AN INCREASINGLY UNSTABLE WORLD

WHITE PAPER / REGULATORY COMPLIANCE READINESS / JUNE 2025

WRITTEN BY RYOMA COLLIA AND EDITED BY GINA COLLIA

TABLE OF CONTENTS

INTRODUCTION

'Hostile cyber activity in the UK has grown more intense, frequent, and sophisticated, with real world impacts for UK citizens.'

Cyber security and resilience policy statement, April 2025.

On 9 April 2025, the UK government published details of the Cyber Security and Resilience Bill (CSRB) that is to be formalised later this year.[1, 2]

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.[3]

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) which EU Member States were required to transpose into their national laws on 17 October 2024.[4, 5]

Current UK NIS regulations are based on the NIS Directive adopted by the European Parliament on 6 July 2016. This Directive has since been superseded in the EU by the NIS2 Directive, which expands the list of critical sectors from seven to eighteen and fills many gaps found within the original regulations. However, in the UK 'Resilience is not improving at the rate necessary to keep pace with the threat', and the CSRB is an urgently required update to UK regulations that will align with NIS2's advancements.

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 infrastructure, resilience, Information Technology (IT), Operational Technology (OT), and services within the scope of requirements.

This paper provides context concerning the importance of the new Bill, information about NIS2 as a founding reference, and key takeaways from the CSRB announcement.

'RESILIENCE IS NOT IMPROVING AT THE RATE NECESSARY TO KEEP PACE WITH THE THREAT'

CYBER SECURITY AND RESILIENCE POLICY STATEMENT, APRIL 2025

THE CYBER CRISIS

Threats from cyberattacks to national infrastructures and the public in general have reached critical levels and 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.[6]

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.[7]

On 4 June 2024, a ransomware attack on Synnovis, a pathology services provider to the NHS, led to significant disruption to NHS services in London. As a result, 10,152 acute outpatient appointments and 1,710 elective procedures were postponed at Guy's and St Thomas' NHS Foundation Trust and King's College Hospital NHS Foundation Trust.[8, 9] Five cases of moderate harm and 114 cases of low harm were reported later that year, followed by reports of two patients showing long-term/permanent damage to their health.[10]

From a financial perspective, the impact of the Synnovis attack is estimated at £32.7M, and the government estimates that, hypothetically, a cyberattack focused on key energy services in the South East of England could wipe over £49 billion from the wider UK economy. The same source states that in the year to September 2024, the National Cyber Security Centre (NCSC) 'managed 430 cyber incidents, with 89 of these being classed as nationally significant–a rate of almost two every week.'[11]

Other examples of high-profile attacks include:

- NCC Group (a UK Government service provider). APT15 (Ke3chang) attack targeting UK government departments and military technology. 2016–2017[12]
- London's Hackney Council. Ransomware attack in October 2020[13]
- Electoral Commission. Cyber-espionage in August 2021[14]
- Russian interference with UK politics and democratic processes. December 2023[15]

In the NCSC Annual Review 2024, the examples shared relating to cyberattack targets are more than sobering: the UK Electoral Commission, UK parliamentarians' emails, industrial control systems, and organisations in the education, finance, healthcare, and defence sectors.[16]

The Cyber Security and Resilience Bill is urgently needed and of critical importance.

THE NETWORK AND INFORMATION SECURITY DIRECTIVE (NIS2)

The EU Network and Information Security Directive (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.

In order to address the shortcomings and cross-border disparities of the basic security and resilience standards of NIS1, NIS2 was developed with a much improved and broader scope.[17] 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. Relevant business entities had to register with a supervisory authority by 17th April 2025. And the requirements apply to businesses outside the EU who have a presence or provide solutions to EU Member States.

SECTORS IN SCOPE OF THE NIS2 DIRECTIVE

NIS2 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

Essential entities (high criticality) are those with 250+ employees, with a €50 million and above annual turnover or a balance sheet of €43 million and above. The sectors are:

- Energy: Electricity, district heating and cooling, oil, gas, and hydrogen
- Transport: Air, rail, water, road
- Banking
- Financial markets infrastructures: Trading venues and central counterparties
- Health: Healthcare providers, reference laboratories, research and development of medicinal products, basic pharmaceutical manufacturing and preparations, medical device manufacturing
- Drinking water
- Waste water
- Digital infrastructure: Internet Exchange Point providers, DNS service providers (excluding operators of root name servers), TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, trust service providers, providers of public electronic communications networks, providers of publicly available electronic communications services
- Information and Communication Technology (ICT) service management (Business-to-Business): Managed service providers and managed security service providers
- Public administration
- Space

Essential entities are those with:

- 250+ employees
- €50M annual turnover and above, or a balance sheet of €43M and above

IMPORTANT ENTITIES

Important entities (other critical sectors) are those with 50+ employees, €10 million and above annual turnover or a balance sheet of €10 million or above. The sectors are:

- Postal and courier services
- Waste management
- Chemicals manufacture, production, and distribution
- Food production, processing, and distribution
- Manufacturing: Medical devices and in vitro diagnostic medical devices, electrical equipment, machinery and equipment, other transport equipment, and computer, electronic, and optical products
- Digital providers: Providers of online marketplaces, online search engines, and social networking services platforms
- Research organisations

Important entities are those with:

- 50+ employees
- €10M annual turnover, or a balance sheet of €10M or above

NIS2 does not take precedence over existing sector-specific compliance requirements, such as the Second Payment Services Directive (PSD2) and Digital Operational Resilience Act (DORA) in the finance sector.

THE THREE PILLARS OF NIS2

ENISA, the European Union Agency for Cybersecurity, has published useful guidance about NIS2, breaking down the basis of the Directive into three basic pillars:[18]

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.[19, 20, 21, 22]
3. Obligations for entities that include cybersecurity risk management measures, incident reporting, and the responsibility of management bodies.

The NCAs facilitate strategic collaboration and cross-Member State information exchange. From a supervisory perspective, they:

- Monitor compliance, carry out on-site inspections and off-site supervision
- Receive incident reports
- Collaborate with CSIRTs on technical responses to incidents
- Collaboratively share information
- Impose supervisory measures and/or enforcement
- Collaborate with Member State authorities

The CSIRTs are also part of the supervisory process, providing operational expertise and assistance. They promote cooperation between Member States to address cross-border incidents, coordinate technical responses, disseminate threat/vulnerability information, and facilitate Member State cooperation.[23]

The EU-CyCLONe supports coordinated operational management in the event of large-scale cybersecurity incidents and crises.

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

To date (27 June 2025), the countries that have successfully enacted NIS2 are Belgium, Croatia, Denmark (partially enacted), Finland, Greece, Hungary, Italy, Latvia, Lithuania, and the Slovak Republic.

Estonia and Portugal have put NIS2 on hold, and all other EU Member States are in the process of enacting it. The EU Commission published a notification on 28 November 2024, stating that enforcement letters were being sent to 23 Member States for remediation.[24]

NIS2 COMPLIANCE REQUIREMENTS AN ALL-HAZARDS APPROACH

The four core elements of the Directive are governance (Article 20), cybersecurity risk management (Article 21), reporting (Article 23), and the use of certified European cybersecurity schemes (Article 24).

1. GOVERNANCE
2. RISK-MANAGEMENT
3. REPORTING
4. CERTIFIED SCHEMES

1. GOVERNANCE

Article 20 states that 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.[25]

The Directive reads, '...management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article' and '...members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.'

2. CYBERSECURITY RISK-MANAGEMENT MEASURES

NIS2 outlines the minimum requirements for compliance in Article 21, stating that:

'Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.'

The Directive goes on to refer to an 'all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents', listing the ten minimum cybersecurity risk-management measures as follows:

- Policies on risk analysis and information system security
- Incident handling
- Business continuity, such as backup management, disaster recovery, and crisis management
- Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
- Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure
- 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 policies, and asset management.
- Multi-factor authentication or continuous authentication solutions, secured voice, video, text communications, and secured emergency communication systems within the entity, where appropriate.

Defining cyber hygiene, Article 49 states that 'Cyber hygiene policies provide the foundations for protecting network and information system infrastructures, hardware, software, and online application security, and business or end-user data upon which entities rely.' Operational Technology (OT)–hardware and software systems that monitor and control physical devices, processes, and infrastructure within industrial environments–is a critical factor, as is the challenge faced by users of legacy systems, which were not created with the levels of cybersecurity needed today.

3. REPORTING

Incident reporting is a core element of NIS2 (Article 23). 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.' (preamble recital 79)

A significant incident is classed as 'an event that has caused/could cause severe operational disruption or financial loss' or one 'that has caused or could cause damage to natural or legal persons.'[26]

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. The CSIRTs and NCAs will respond to the entity, and a summary report is sent to ENISA every three months by a single point of contact from the NCA or CSIRT. The CSIRTs and NIS Cooperation Group provide observations and findings every six months.

4. USE OF EUROPEAN CYBERSECURITY CERTIFICATION SCHEMES

Article 24 states that 'Member States may require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of the [European Cyber Resilience Act].[27] Furthermore, Member States shall encourage essential and important entities to use qualified trust services.

The ISO/IEC 27000 series is mentioned as an example during the preamble (recital 79). The British Standards Institute has published a paper on NIS2 compliance and ISO 27001 and ISO 22301.[28] ISO 27001 facilitates NIS2 compliance by adopting "appropriate and proportionate" technical and organisational measures. ISO 22301 is 'recommended for business continuity management, assisting in implementing, maintaining, and continuously improving business continuity practices.'

Dejan Kosutic, CEO of Advisera, is a specialist in ISO standards, EU regulations, and specialist documentation. He ran an analysis comparing ISO 27001 and NIS2, finding that ISO 27001 can address 25 of the 26 requirements covered by Articles 20 and 21 (Governance and Cybersecurity Risk-Management Measures). The only exception is crisis management. It is not covered in ISO 27001.

The table below containing Dejan's valuable analysis is shared with his kind consent. The original findings are here.

NIS 2 Requirement	NIS 2 Article	ISO 27001 Clause or Control
Management bodies must oversee the implementation of cybersecurity risk-management measures.	Article 20(1)	9.1 Monitoring, measurement, analysis, and evaluation. 9.2 Internal audit. 9.3 Management review.
Members of management bodies are required to follow training, and must offer similar training to their employees on a regular basis.	Article 20(2)	7.2 Competence A.6.3 Information security awareness, education, and training.
Entities must take appropriate and proportionate technical, operational, and organizational measures to manage the risks.	Article 21(1)	6.1.3 Information security risk treatment. 6.2 Information security objectives and planning to achieve them 8.1 Operational planning and control.
When assessing the proportionality of measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size, and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.	Article 21(1)	6.1.2 Information security risk assessment.
Policy on risk analysis.	Article 21(2), point (a)	6.1.2 Information security risk assessment.
Policy on information system security.	Article 21(2), point (a)	5.2 Policy.
Incident handling.	Article 21(2), point (b)	A.5.24 Information security incident management planning and preparation. A.5.25 Assessment and decision on information security events. A.5.26 Response to information security incidents.
Business continuity.	Article 21(2), point (c)	A.5.29 Information security during disruption.
Backup management.	Article 21(2), point (c)	A.8.13 Information backup.
Disaster recovery.	Article 21(2), point (c)	A.5.30 ICT readiness for business continuity. A.8.14 Redundancy of information processing facilities.
Crisis management.	Article 21(2), point (c)	Does not have a directly relevant clause or control in ISO 27001.
Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.	Article 21(2), point (d)	A.5.19 Information security in supplier relationships. A.5.20 Addressing information security within supplier agreements. A.5.21 Managing information security in the ICT supply chain. A.5.22 Monitoring, review, and change management of supplier service. A.5.23 Information security for the use of cloud services.
Security in network and information systems acquisition, development, and maintenance.	Article 21(2), point (e)	A.8.6 Capacity management. A.8.7 Protection against malware. A.8.8 Management of technical vulnerabilities. A.8.9 Configuration management. A.8.25 Secure development life cycle. A.8.26 Application security requirements. A.8.27 Secure system architecture and engineering principles. A.8.28 Secure coding. A.8.29 Security testing in development and acceptance. A.8.30 Outsourced development. A.8.31 Separation of development, test, and production environments. A.8.32 Change management. A.8.33 Test information.

NIS 2 Requirement	NIS 2 Article	ISO 27001 Clause or Control
Policies and procedures to assess the effectiveness of cybersecurity risk-management measures.	Article 21(2), point (f)	9.1 Monitoring, measurement, analysis, and evaluation. 9.2 Internal audit. 9.3 Management review.
Basic cyber hygiene practices.	Article 21(2), point (g)	A.6.8 Information security event reporting. A.7.7 Clear desk and clear screen. A.7.9 Security of assets off-premises. A.7.10 Storage media. A.8.1 User endpoint devices. A.8.5 Secure authentication. A.8.7 Protection against malware. A.8.13 Information backup. A.8.19 Installation of software on operational systems. A.8.24 Use of cryptography.
Cybersecurity training.	Article 21(2), point (g)	7.2 Competence. A.6.3 Information security awareness, education, and training.
Policies and procedures regarding the use of cryptography and encryption.	Article 21(2), point (h)	A.8.24 Use of cryptography
Human resources security.	Article 21(2), point (i)	A.6.1 Screening. A.6.2 Terms and conditions of employment. A.6.3 Information security awareness, education, and training. A.6.4 Disciplinary process. A.6.5 Responsibilities after termination or change of employment.
Access control policies.	Article 21(2), point (i)	A.5.15 Access control.
Asset management.	Article 21(2), point (i)	A.5.9 Inventory of information and other associated assets. A.5.10 Acceptable use of information and other associated assets. A.5.11 Return of assets. A.7.9 Security of assets off-premises.
The use of multi-factor authentication or continuous authentication solutions.	Article 21(2), point (j)	A.5.16 Identity management. A.5.17 Authentication information. A.8.5 Secure authentication.
Secured voice, video, and text communications.	Article 21(2), point (j)	A.5.14 Information transfer. A.8.21 Security of network services.
Secured emergency communication systems within the entity.	Article 21(2), point (j)	A.8.20 Network security.
Take into account the vulnerabilities specific to each direct supplier and service provider, and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.	Article 21(3)	A.5.19 Information security in supplier relationships. A.5.21 Managing information security in the ICT supply chain. A.5.22 Monitoring, review, and change management of supplier service. A.5.23 Information security for use of cloud services.
Take appropriate and proportionate corrective measures.	Article 21(4)	10.2 Nonconformity and corrective action.

SUPPLY CHAIN SECURITY

Playing an important part in the Member States' cybersecurity strategy, 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.'[29]

Preamble recital 85 states:

'Addressing risks stemming from an entity's supply chain and its relationship with its suppliers, such as providers of data storage and processing services or managed security service providers and software editors, is particularly important given the prevalence of incidents where entities have been the victim of cyberattacks and where malicious perpetrators were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third-party products and services. Essential and important entities should therefore assess and take into account the overall quality and resilience of products and services, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures. Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers. Those entities could consider risks stemming from other levels of suppliers and service providers.'

Further, preamble recital 90 recommends that entities should carry out coordinated security risk assessments of critical supply chains with the aim of 'identifying, per sector, the critical ICT services, ICT systems or ICT products, relevant threats and vulnerabilities.'

It then states that coordinated security risk assessments should identify:

- Measures
- Mitigation plans
- Best practices to counter:
- Critical dependencies
- Potential single points of failure
- Threats
- Vulnerabilities and other risks associated with the supply chain

The Directive includes three mechanisms to manage supply chain compliance: EU level coordinated security risk assessments (Article 22(1)); empowering EU Member States to extend the scope of the Directive to entities outside the Directive's original scope (various references within the Directive); and obligations provided for in the requirement for supply chain security to be extended to 'security-related aspects concerning the relationships between each entity and its direct suppliers or service providers' (Article 21(2d)).

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 are detailed in Articles 32 and 33. These 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

Fines

Essential Entities

€10,000,000 or of a maximum of at least 2 % of the total worldwide annual turnover

Important Entities

€7,000,000 or of a maximum of at least 1.4 % of the total worldwide annual turnover

Enforcement Powers

- Violations made public
- Temporary suspension of services
- Personal Liability
  - Public naming of responsible persons
  - Temporary ban for individuals from holding management positions

THE UK CYBER SECURITY AND RESILIENCE BILL (CRSRB)

In the CSRB announcement in April, the government stated its intention to 'address the specific cyber security challenges faced by the UK while aligning, where appropriate, with the approach taken in the EU NIS 2 directive.' As mentioned above, the current UK NIS regulations are based on the NIS Directive adopted by the European Parliament on 6 July 2016. These basic and limited regulations were implemented in the UK in 2018 and have remained the UK's only cross-sector cybersecurity legislation. Aligning with the much expanded NIS2 Directive and adding further UK-specific requirements will be a significant step forward in protecting the UK from cyber threats.

The CSRB will be introduced to Parliament later this year. In the meantime, the policy statement provides details of measures we should expect to see.

Bringing More Entities into Scope of the Regulatory Framework

Very much in line with EU findings relating to cybersecurity and resilience risks in the supply chain, 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.

The following measures are outlined in the policy statement.

1 Bringing More Entities into Scope of the Regulatory Framework

Very much in line with EU findings relating to cybersecurity and resilience risks in the supply chain, 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.

The following measures are outlined in the policy statement.

1.1 Managed Service Providers (MSPs)

MSPs have been specifically named as playing a critical role in the resilience of IT systems, networks, infrastructure, and data. The Cloud Hopper attack on MSPs and the attack on the Ministry of Defence's personnel system are used as an example.[30, 31]

The policy statement defines a managed service 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.[32]

1.2 Strengthening Supply Chain Security and Enabling Regulators to Designate 'Critical Suppliers'

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.[33]

The new Bill sets out to tackle this, focusing on operators of essential services (OES) and relevant digital service providers (RDSP) in secondary legislation. 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.

2 Empowering Regulators and Enhancing Oversight

In order to empower regulators, the government outlined the following measures that will provide a framework, appropriate mechanisms, and enhanced oversight.

2.1 Technical and Methodological Security Requirements: The NCSC Cyber Assessment Framework (CAF)

The policy statement outlines the UK Government's intention to establish best practices based on the NCSC Cyber Assessment Framework (CAF).[34] The CAF is a collection of cybersecurity principles and objectives available online to help organisations assess and manage their cybersecurity.

Divided into four objectives, the CAF covers: managing security risk, protecting against cyberattacks, detecting cybersecurity events, and minimizing the impact of cybersecurity incidents.

2.2. Improved Incident Reporting

Under current UK regulations, an incident is only reportable in the event of an interruption in essential or digital services, leaving many incidents unreported and limiting the ability of regulators to identify vulnerabilities. The new Bill will expand reporting criteria and transparency requirements, update incident reporting timelines, and streamline reporting.

The UK NIS regulations' supervisory authorities include the Information Commissioner's Office and twelve UK supervising bodies relating to the five specific sectors (energy, transport, health, drinking water supply and distribution, and digital infrastructure) that are currently in scope.[35]

As the CSRB will be expanding the number of entities in scope, the number of supervisory authorities will likely increase to oversee the additional sectors.

2.3 Expansion of the Information Commissioner's Office's Information Gathering Powers

Currently, the role of the Information Commissioner's Office (ICO) as a regulator for Relevant Digital Service Providers (RDSPs) is reactive rather than proactive. The new Bill will change this, empowering the ICO to identify the most critical entities that fall under the regulatory remit and expanding its enforcement powers.

2.4 Improved Regulators' Cost Recovery Mechanisms

Current regulations limit the ability of regulators to recover costs, thereby creating cash flow challenges. The new Bill will enable regulators to apply new fee regimes and mechanisms to cover the costs of regulation and enforcement.

3 Delegated Powers – Ensure the Regulatory Framework is Adaptable to Emerging Threats

The cyber landscape is ever-changing and evolving. Building a flexible regulatory framework that is adaptable to emerging threats is essential. The new Bill will delegate powers that enable agile regulations.

The powers sought by the government would enable regulatory updates without an Act of Parliament, including the ability to add new sectors and sub-sectors in scope, subject to safeguards.

ADDITIONAL MEASURES UNDER CONSIDERATION

The policy statement includes additional measures for consideration to address the ever-evolving threat landscape and states that the government will consider the most appropriate legislative vehicle for the following:

1 Bringing Data Centres into Scope of the Regulatory Framework

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.

2. Publish a Statement of Strategic Priorities for Regulators

In line with other regulatory regimes, such as telecoms and online safety, the government is considering the introduction of a new power for the Secretary of State to publish a Statement of Strategic Priorities. This establishes a unified set of objectives and expectations for the implementation of the regulations.

3. Powers of Direction

Surprisingly, the UK government does not currently have the power to issue directions to regulated entities. New executive powers have been proposed to address this which would empower the government to execute 'swift and decisive action', including direct intervention, in response to cyber threats that may impact the nation's security and infrastructure.

CONCLUSION

As the Right Honourable Peter Kyle MP, Secretary of State for Science, Innovation and Technology, points out in the ministerial foreword to the cyber security and resilience policy statement:

'The first duty of this government is to keep its citizens safe. To anticipate the threats we face, minimise the risks we take, and make the UK as safe and secure as it can possibly be. That is what making National Security our number one priority means in practice.'

We live in an increasingly unstable world, and each and every day the risk posed by cyber criminals and hostile states grows. An update to current UK legislation is long overdue and should be welcomed by all. The threat will not abate and should not be underestimated; cyber criminals are constantly adapting to increase the effectiveness of their attacks. The CSRB, like NIS2, aims to address this risk and provide effective and enduring protection for our Critical National Infrastructure and our essential public services.

NOTES

Key to frequently used sources:

CSRB: UK Cyber Security and Resilience Policy statement
ENISA: The European Union Agency for Cybersecurity.
NIS: The Network and Information Systems Regulations 2018
NIS2: EU Network and Information Security Directive (2022) - EU Directive 2022/2555

1 CSRB policy statement was published on 9th April 2025.
2 New cyber laws to safeguard UK economy and secure long-term growth.
3 Critical National Infrastructure. National Infrastructure: those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends.
4 NIS.
5 NIS2.
6 2024 Thales Data Threat Report.
7 Cyber security breaches survey 2024.
8 NHS England: Synnovis cyber incident.
9 Synnovis cyber incident update.
10 Ibid.
11 New cyber laws to safeguard UK economy and secure long-term growth.
12 NCC Group: APT15 is Alive and Strong.
13 Information Commissioner's Office: London Borough of Hackney reprimanded following cyber-attack.
14 Electoral Commission: Information about the cyber-attack.
15 UK exposes attempted Russian cyber interference in politics and democratic processes.
16 National Cyber Security Centre Annual Review 2024
17 Ibid., NIS.
18 ENISA.
19 NIS Cooperation Group.
20 CSIRTs, Computer Security Incident Response Teams Network Network.
21 EU CyCLONe, European Cyber Crisis Liaison Organisation Network.
22 EUVD, EU Vulnerability database.
23 Ibid., ENISA.
24 Commission takes action to ensure complete and timely transposition of EU directives.

Continued...

ENDNOTES

25 Ibid., NIS2, Article 20.
26 Ibid., ENISA Incident Reporting Obligations.
27 European Cyber Resilience Act Regulation EU 2019/881.
28 The British Standards Institute: What is the NIS2 Directive?
29 NIS2, Preamble recital 91.
30 Operation Cloud Hopper.
31 Chatham House: MOD data breach.
32 Ibid., CSRB, Section 1.2.2.
33 Ibid., CSRB, Section 1.2.1.
34 Cyber Assessment Framework (CAF).
35 NIS, Schedule 1, Regulation 3.

ABOUT THE AUTHOR AND THE EDITOR

Ryoma (Ray) Collia is a writer and commercial business consultant who has spent over eighteen years working in clinical trials and life sciences and over thirty years working in technology, data management, regulatory compliance, and supply chain across multiple sectors.

Gina Collia is a professional researcher, writer, editor, and publisher with decades of experience. Her work can be found in leading Universities, museums, libraries, associations, and collections globally.

Together, we specialise in business communication, particularly long-form content that translates complex ideas, texts, and messaging into clear, accessible thought-leadership, education, and guidance.

If you'd like to learn more, just contact us here.

WEBSITE

www.wordferret.co.uk

EMAIL

contact@wordferret.co.uk

ADDRESS

Word Ferret
Queensgate House,
48 Queen Street,
Exeter,
Devon,
EX4 3SR,
United Kingdom

UK PHONE OR WHATSAPP

+44 7789 721821