People powered, tech-enabled cyber security

FOX IT
part of nccgroup

Global Cyber Policy Radar:

Report on Cyber Security Regulation Trends

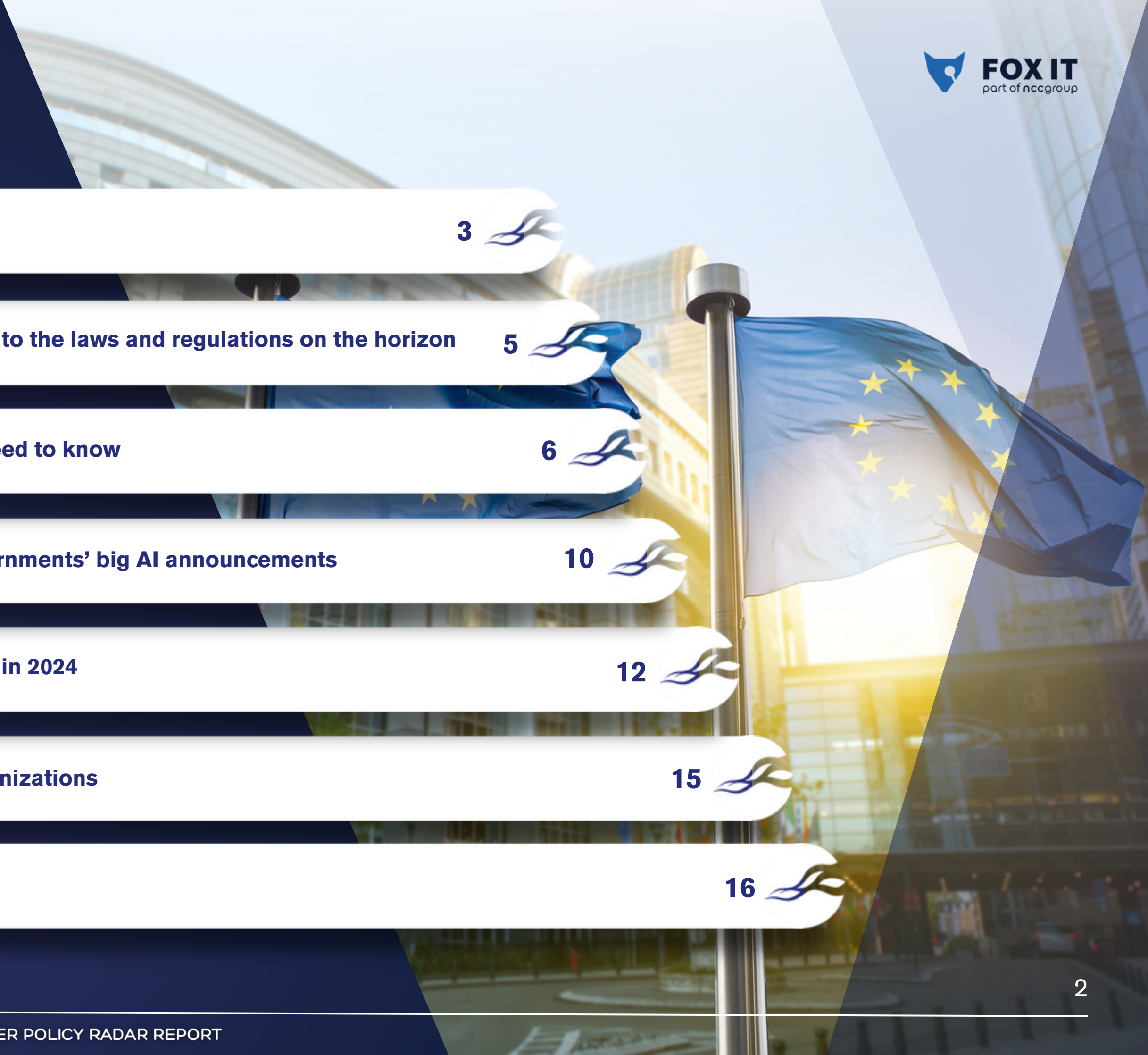
What's inside

- Navigate Global Cyber Security Laws
- Insights from Experts in Government Policy
- Recommendations for your Regulatory Compliance

Edition 1

FEBRUARY 2024 | GLOBAL CYBER POLICY RADAR REPORT

Contents



Introduction

Welcome to NCC Group's inaugural Global Cyber Policy Radar Report.

NCC Group is proud to be a close advisor to governments and legislators globally as they make important decisions about the future of cyber rules. Utilizing our deep technical expertise, we help to shape new laws and policies. We do so with the aim of creating a conducive operating environment and delivering on our purpose to create a more secure digital future.

Where we operate, whether that is in the UK, the Netherlands and across Europe, North America, Australia or Singapore, our engagement with cybersecurity policymakers also affords us unique insights into the key regulatory and legislative changes affecting us and our clients, and the commonalities and differences they need to navigate around the world. This report draws from these insights, and our wider work helping clients track key developments, covering:

- Our Regulation Radar looking to the laws and regulations on the horizon
- The recent policy developments you need to know
- A spotlight on AI safety regulation
- The three things to look out for in 2024

We are confident that our Global Cyber Policy Radar Report is a valuable resource for anyone across the cyber ecosystem who needs to make sense of the ever-evolving global cyber policy landscape.

Verona Johnstone-Hulse
UK Head of Government Affairs
An experienced government affairs and policy professional, Verona oversees NCC Group's engagement with UK government and regulatory decision-makers and the wider policymaking community, against a backdrop of the increasing regulation of cyber resilience.

Kat Sommer
Group Head of Government Affairs & Analyst Relations
Seeking to act as an interpreter between technical, policy and analyst communities, Kat leads NCC Group's political engagement, government relations and lobbying work, educating policy-makers.

Willemijn Rodenburg
Relationship Manager Government NL (Fox-IT and Fox Crypto)
With over 15 years' experience in the Dutch Central Government, Willemijn is currently responsible for managing key stakeholder relationships and public affairs within the Dutch Government.

At a glance

Need to know

1. While politics may have delayed some reforms, cyber rules for critical infrastructure continue to be tightened and more widely applied.
2. Governments told us not to pay ransomware gangs. But stopped short of an outright ban – for now.
3. Governments are making moves to assure the quality of services provided by practitioners and cyber firms.

Look out for

1. Elections = policy hiatus? Cyber practitioners should be conscious of the effect the elections are likely to have on cyber lawmaking.
2. Incident reporting requirements are set to strengthen further over the coming months.
3. Governments will be pursuing a mix of mandatory and voluntary measures to enhance hardware and software security standards.

Typical sectors that fall in scope across the regulatory frameworks

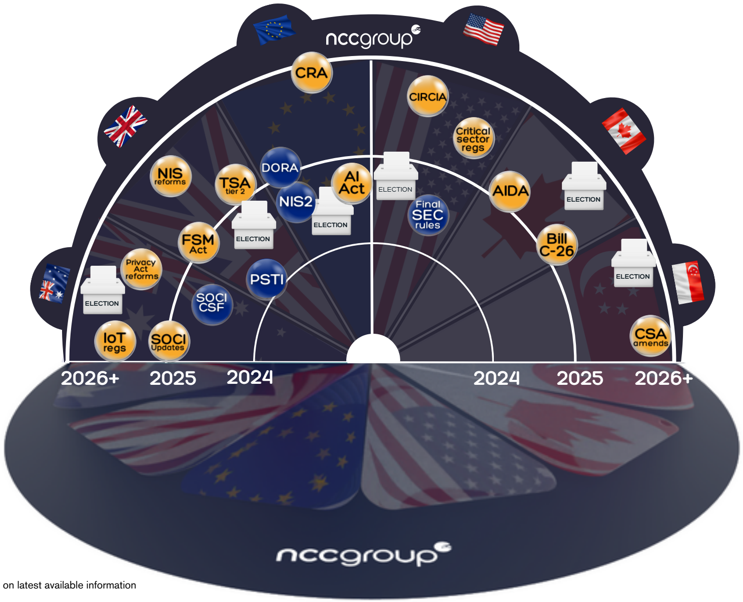
- Energy
- Transport
- Banking/Finance
- Health
- Water
- Digital Infrastructures
- Public Administration
- Space
- Postal & Courier services
- Waste Management
- Chemical Products
- Food
- Manufacturers
- Digital Providers
- Research Organizations

How could your organization be impacted?

FIND OUT MORE

Regulation Radar

The key laws and regulations on the horizon that will introduce additional cyber security requirements.



ELECTION **National Election**

🟠 **Implementation date TBC**

🔵 **Implementation date confirmed**

Timelines represented here reflect NCC Group's estimations, based on latest available information

Australia
IoT regs - Plans to legislate for a mandatory cyber security standard for Internet of Things devices
SOCI - Security of Critical Infrastructure Act
SOCI CSF – Grace period for compliance with SOCI cyber security framework in part 2a ends
Privacy Act – reforms expected following 2023 review

United Kingdom
FSM Act - Financial Services and Markets Act 2023
NIS - The Security of Network & Information Systems Regulations
PSTI - Product Security and Telecommunications Infrastructure Act 2021
TSA - Telecommunications (Security) Act 2021

Europe
AI Act - Artificial Intelligence Act
CRA - Cyber Resilience Act
DORA - Digital Operational Resilience Act
NIS2 - DIRECTIVE (EU) 2022/2555

United States
CIRCIA - Cyber Incident Reporting for Critical Infrastructure Act
SEC rules - Security Exchange Commission's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rules
Critical sector regs - Federal Government to harmonize cyber security regulations for critical sectors

Canada
AIDA - Artificial Intelligence and Data Act
Bill C-26 - Draft critical infrastructure cyber security law

Singapore
CSA - (Singapore) Cybersecurity Act

1

Policy developments you need to know

While politics may have delayed some reforms, cyber rules for critical infrastructure continue to be tightened and more widely applied.

EU Member States are moving forward with implementing the NIS2 Directive ahead of the October 2024 transposition deadline, with draft Bills/proposals published in Germany, France and Sweden (among others). In the Netherlands, national legislation has been postponed to the end of 2024. The EU Commission, meanwhile, has issued guidance on the interplay between NIS2 and existing sector-specific laws, requiring Member States to introduce additional obligations where existing laws do not meet the high bar set in NIS2.

The UK previously announced updates to its own NIS regulations, extending the requirements to new sectors like energy flexibility providers and managed service providers. But the current Government has delayed the necessary legal reforms, choosing to use the remaining time it has left before the next General Election (expected in 2024) to pursue more voter-facing laws. In the meantime, the Cyber Assessment Framework (CAF) continues to be rolled out across existing regulated sectors.

In the absence of any legislative levers, the U.S. Federal Government is using “existing authorities” to set and harmonize cyber security requirements across critical sectors (based on NIST’s CSF 2.0 and CISA’s Cyber Security Performance Goals) and provide further support to Sector Risk Management Authorities (SRMAs) to implement the reforms. Foreign suppliers to critical infrastructure will also be encouraged to adopt NIST C-SCRM best practices. Meanwhile, the Security Exchange Commission’s (SEC) new incident and annual reporting requirements for public companies came into effect for most companies in December 2023.

Both the EU and UK have published more details on their plans to regulate the resilience of financial services through DORA and the Financial Services and Markets (FSM) Act. Notably, in a further widening of the net of cyber regulations, both regimes will place requirements on critical suppliers.

Need support preparing for new and evolving critical infrastructure cyber regulations?

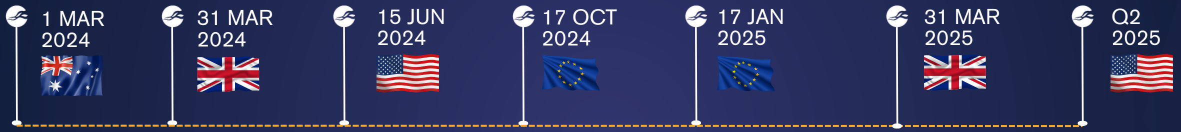
FIND OUT MORE

Policy developments you need to know

The Australian Federal Government has announced plans to extend the SOCI Act to include telecoms providers, implement new cyber rules for maritime and aviation, and require "Systems of National Significance" to face additional cyber security obligations such as developing cyber incident response plans, undertaking cybersecurity exercises and conducting vulnerability assessments.

Canada's C-26 Bill - which would establish a regulatory framework to strengthen baseline cybersecurity for operators of services and systems that are vital to national security and public safety – remains in Parliament, with Committee hearings recently opening on the draft law.

The Cybersecurity Agency of Singapore is reviewing plans to update its Cybersecurity Act (CSA) to keep pace with modern technology developments, extend the scope of requirements to new sectors of the economy, and enhance reporting requirements.



1 MAR 2024

Consultation on reforms to SOCI Act closes

31 MAR 2024

Tier 1 operators under UK TSA required to implement first set of measures

15 JUN 2024

Smaller companies required to comply with SEC reporting rules

17 OCT 2024

Member States required to implement NIS2

17 JAN 2025

DORA will apply. NIS2 regulated entities required to submit information to competent authorities

31 MAR 2025

Tier 2 operators under UK TSA required to implement first set of measures

Q2 2025

U.S. Federal Government to have set cyber security regulations for critical sectors

Policy developments you need to know

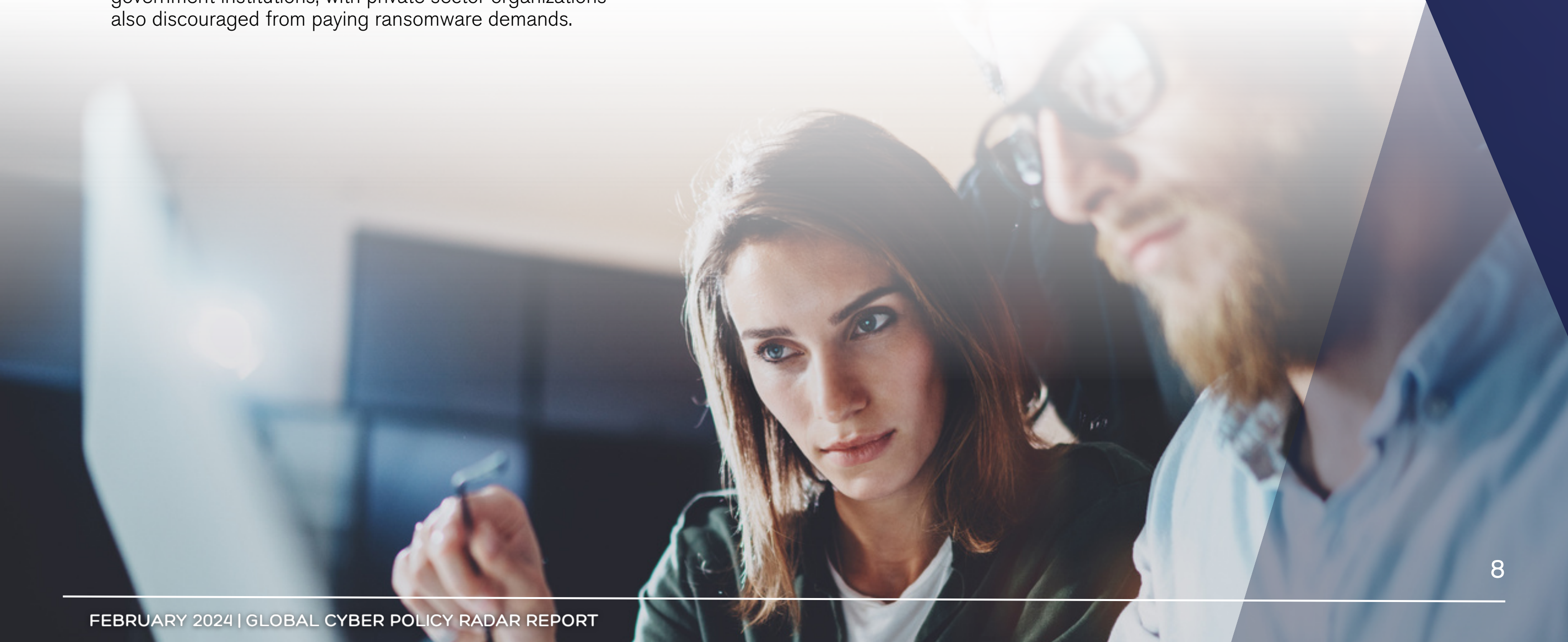
2

Governments told us not to pay ransomware gangs. But stopped short of an outright ban – for now.

After consulting on potential plans to stop ransomware payments, the Australian Government decided not to move ahead with an outright ban. Instead, the Government, in their new 2023-2030 Cyber Security Strategy, "strongly discourages" paying ransoms to cybercriminals.

Governments are leading from the front, with 48 countries, the EU and INTERPOL signing up to a pledge not to pay ransoms at the third Annual Meeting of the International Counter Ransomware Initiative (CRI). The pledge covers government institutions, with private sector organizations also discouraged from paying ransomware demands.

We have also seen good progress through the CRI to develop global capabilities, share information and stop illicit flow of funds through shared blacklisting initiatives and cryptocurrency tracking. Having long-advocated for governments to use all the statecraft tools at their disposal to tackle ransomware, both in our evidence to the UK Parliament and in our engagement with the Australian Federal Government, NCC Group is very pleased to see such progress through the CRI.



Policy developments you need to know

3

With the cyber industry an increasingly critical pillar of the digitalized economy, governments are making moves to assure the quality of services provided by practitioners and cyber firms.

Australia has announced plans to co-design a code of practice for incident response providers, defining the service quality and professional standards that are expected from third-party cyber incident response providers. More broadly, it is working with industry to develop a cyber skills framework that aims to provide assurance to employers that its cyber workforce is appropriately skilled, and workers that their qualifications and relevant experience are recognized and fit-for-purpose. We are also starting to see requests for appropriately qualified individuals to undertake Essential Eight assessments.

The first professional 'Charterships' have been awarded through the UK Cyber Security Council, the UK cyber industry's self-regulatory body. The UK Government previously indicated that it would drive uptake of the Charterships through public sector procurement, while conversations with UK regulators about increasing uptake in critical sectors like energy and financial services have started.

In a bid to harmonize requirements across borders, Singapore and the UK are exploring opening up the UK Cyber Security Council Charterships to practitioners in Singapore, something NCC Group has advocated for, including through our participation in the recent UK-Singapore Cyber Dialogue.

The EU is moving forward with Europe-wide certification schemes for managed security services, through amendments to the Cybersecurity Act (CSA). This comes as the recently introduced Cyber Solidarity Act aims to establish a 'Cyber Reserve' of security providers that can be accessed in the event of a large scale cyber incident.

In spotlight: Decoding governments’ big AI announcements

NCC Group’s Chief Scientist Chris Anley has been supporting and engaging with legislators as they develop and announce new policies and regulations on AI safety. Here he provides his insights on what to expect from governments globally following a busy few months of summits and flagship announcements:

Governments don’t want AI developers to assure their own systems - or, as the UK Prime Minister put it, “we should not rely on them marking their own homework.” The need for safety testing features in the Bletchley Declaration – the high-level statement of intent from 28 countries (including, most notably, the U.S. and China) to develop safe and responsible frontier AI. Meanwhile, new G7 guidance emphasises that testing should include both “internal and independent external testing measures” as well as “a combination of methods such as red teaming.” Indeed, third party assurance of high-risk AI systems looks set to be required across most major economies’ domestic regulatory frameworks.

There are positive signs of global cooperation on what is, ultimately, a global issue. The Bletchley Declaration should not only be applauded for its diverse range of signatories but also its commitments to keep the conversation going through two further AI Safety Summits in South Korea and France in 2024. While we must be realistic about what can be achieved across this many nation states, clarity of mission and measurable targets that leaders can track progress against will help to ensure the continued success of these international gatherings.

Chris Anley
Chief Scientist
Chris has been carrying out security audits since 1996, performing thousands of penetration tests, code reviews and design reviews on a wide variety of platforms, languages and architectures for many of the world's largest companies.

In spotlight:
Decoding governments' big AI announcements

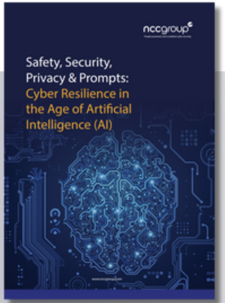
There will be regulation. Governments globally have either announced or are developing plans to embed these safety and security principles in domestic regulation. That said, governments are taking different stances on the exact shape of these regulations and the timescales they are working to. For example:

- The White House's Executive Order (EO 14110) marks a real step change in the U.S.'s approach to safeguarding AI, with Vice President Harris calling for legislation and arguing that "history has shown in the absence of regulation and strong government oversight, some technology companies choose to prioritize profit over the wellbeing of their customers, the security of our communities and the stability of our democracies." In a recent progress update, the White House stated that Federal Agencies are using the Defense Production Act authorities to compel developers of the most powerful AI systems to report vital information, especially AI safety test results, to the Department of Commerce.
- Despite significant discussion and pushback against its plans to explicitly prohibit the development of very high-risk AI systems, it now looks likely that the EU AI Act will pass before the European Parliament elections. When introduced, the Act will establish significant requirements for the developers and users of AI systems.
- The UK has reaffirmed its commitment to a principles-based sector-specific approach to regulation within its current legal framework, while also announcing plans to consult on the risks presented by highly-capable, general purpose AI models and whether further legislation is suitable in the short term.
- Australia has announced plans to consult on mandatory safeguards for those who develop or deploy AI systems in legitimate, high-risk settings.

For further reading on this topic, NCC Group's recent Whitepaper

Safety, Security, Privacy & Prompts: Cyber Resilience in the Age of Artificial Intelligence

Seeks to set a baseline of understanding for some of the key AI concepts, threats and opportunities, supporting business decision makers' thinking and strategies in this fast-paced, exciting new technological era.



nccgroup

Safety, Security, Privacy & Prompts: Cyber Resilience in the Age of Artificial Intelligence (AI)

DOWNLOAD

Three things to look out for in 2024

1

Elections = policy hiatus?

With 40 countries going to the polls in 2024, electoral integrity in the face of emerging tech and nation-state cyber threats will be high on every cyber practitioner's radar (as we explored in our 2024 outlook piece here). However, another development practitioners should be conscious of is the effect the elections are likely to have on cyber lawmaking.

In the EU, we are waiting to see whether crucial laws such as the Cyber Solidarity Act, AI Act and Cyber Resilience Act are enacted in the remaining time before the June elections. In the UK, the Government has all but accepted that it does not have enough parliamentary time to pass new cyber laws, with officials now focusing their efforts on alternative ways to drive up cyber resilience such as through government procurement and voluntary measures. This includes a new voluntary Cyber Governance Code of Practice aimed at formalising Government's expectation of Company Directors managing cyber risk.

Cyber watchers will also want to keep an eye out for the new programmes of government following the elections. While we're not expecting cyber security to be a major election issue (unless wider events drive the issue up the political agenda), we do expect the broad trend toward the greater regulation of cyber security to be reflected across new governments' policy programmes – with cyber security standards supported across the political divide in most jurisdictions.

NCC Group's Government Affairs team attended the UK's two main political parties' 2023 annual conferences and got under the skin of what a Conservative or a Labour Party 'programme for government' could say about technology, cyber resilience, and the future digital economy. Read their report back here:

Where is Cyber Policy Headed in the UK?
A report back from the 2023 political party conferences

READ THE REPORT

Three things to look out for in 2024

2

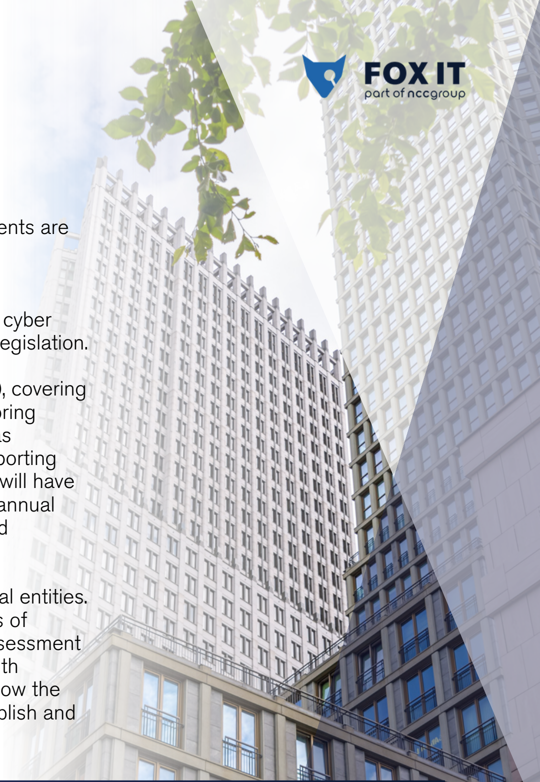
Incident reporting mandates

Partially reflective across increased critical infrastructure regulation, incident reporting requirements are set to strengthen over the coming months.

The Australian Government has announced plans to introduce a mandatory no fault, no liability ransomware reporting obligation, with a view to improving its understanding of ransomware and cyber extortion trends. The Government plans to work with industry to co-design possible options for legislation.

U.S. agency CISA has confirmed that it will publish the Notice of Proposed Rulemaking (NPRM), covering how it will implement the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), by Spring 2024. The new incident and ransom payment reporting requirements for critical infrastructure, as introduced by CIRCIA, will be finalised 18 months thereafter. Meanwhile, SEC's new incident reporting rules came into effect in December 2023 for larger public companies, while smaller registrants will have to comply from June 2024. The new rules also put company boards firmly in the spotlight, with annual reporting obligations including the requirement to disclose a board's cyber security expertise and oversight of cyber risks.

Finally, the EU's NIS2 Directive and DORA introduce enhanced reporting requirements for critical entities. For NIS2 entities, this includes a new 3-tier reporting system: an "early warning" within 24 hours of becoming aware of the incident; an "incident notification" within 72 hours, providing an initial assessment of the incident's severity, impact and indicators of compromise; and, a "final report" within 1 month covering a detailed description including the incident's root cause. We may see more detail on how the new 3-tier reporting system will be implemented over the coming months as Member States publish and pass their regional laws transposing the Directive.



1 MAR 2024 — Consultation on a mandatory ransomware reporting obligation closes

MAR 2024 — CISA to publish CIRCIA NPRM

15 JUN 2024 — Smaller companies required to comply with SEC reporting rules

17 OCT 2024 — Member States required to implement NIS2

17 JAN 2025 — DORA will apply

Three things to look out for in 2024

3

New standards for hardware and software

All eyes will be on the EU's Cyber Resilience Act (CRA) which, amidst some opposition by the security community, is set to be adopted shortly. The new law will introduce cybersecurity requirements for a significant proportion of hardware and software sold into the EU, covering risk assessments, vulnerability handling processes, and incident reporting. Once adopted, manufacturers and developers will have 36 months to adapt to the new requirements, with the exception of a more limited 21-month grace period in relation to the reporting obligations. This comes as the European Commission has adopted the implementing regulation for the (currently) voluntary Common Criteria-based cybersecurity certification scheme (EUCC).

Outside of the EU, governments will be pursuing a mix of mandatory and voluntary measures to enhance hardware and software security standards:

Manufacturers of consumer Internet of Thing (IoT) devices must comply with the requirements set out in the UK Product Security and Telecoms Infrastructure (PSTI) Act by April 2024. In absence of any time to legislate before the next election, the UK Government is crafting and driving the uptake of Codes of Practices for Apps and App Stores and software security. While these Codes are voluntary at this stage, as we have seen with the PSTI consumer IoT requirements, such Codes could be mandated in the long term.

The Australian Government has announced that it will legislate for a mandatory cyber security standard for IoT devices, supported by a voluntary smart device labelling scheme for consumer devices. Like the UK, it also plans to develop a voluntary Code of Practice for Apps and App Stores, while working to harmonise software standards on the international stage.

In the U.S., the Federal Government is using its procurement levers to drive up standards, implementing new procurement rules on IoT cyber security alongside a Government IoT security labelling program. It is also exploring approaches to develop a software liability framework, while CISA is leading a public-private partnership to develop and drive adoption of secure-by-design and secure-by-default principles for hardware and software that will be completed by the end of 2024.

1 MAR 2024
Consultation on Australian mandatory IoT standards closes

29 April 2024
PSTI Act to come into effect

Q2 2024
U.S. to explore software liability framework

End of 2024
CISA drive to adopt secure-by-design and secure-by-default principles

H2 2025
CRA vulnerability reporting requirements likely to come into effect

H1 2027
CRA essential cyber security requirements likely to come into effect

Key considerations for organizations

1 Increasing cyber regulation is the talk of the town. Don't wait until the compliance deadline looms to take action.

2 Boards are increasingly held accountable for cyber compliance. Make sure your executives have the information they need to make decisions about your cyber strategy.

3 Know how to use policy insights and political horizon-scanning to inform sustainable cyber investments.

4 Know the right questions to ask to ensure your decisions are future-proof in light of ever changing regulatory and political developments.

5 Compliance doesn't always equal good security. Know the difference.

6 Gain a better understanding of the regulatory complexity and the decisions you can take to avoid fragmentation.

Glossary

Australia	**Essential Eight** A baseline cyber threat mitigation strategy set out by the Australian Signals Directorate. **Privacy Act** The Australian Government has announced plans to further strengthen the Privacy Act, with draft legislation (subject to consultation) due to go before Parliament in 2024. **SOCI** Security of Critical Infrastructure Act – Australia's law governing the cybersecurity of critical infrastructure. **SOCI CSF** Grace period for compliance with SOCI cyber security framework in part 2a ends in August 2024
United Kingdom	**CAF** Cyber Assessment Framework. **FSM Act** Financial Services and Markets Act 2023 – UK law introducing, among other things, a new regulatory regime for critical suppliers to the financial sector. **NIS** The Security of Network & Information Systems Regulations – UK regulation setting security requirements for essential and digital services. (NB. The Network & Information Systems (NIS) Directive has now been superseded by NIS2 in the EU.) **PSTI** Product Security and Telecommunications Infrastructure Act 2021 – The UK law implementing minimum cybersecurity requirements for consumer connectable devices. **TSA** The UK Telecommunications (Security) Act 2021 places cyber security requirements on telecoms operators.
Europe	**AI Act** Artificial Intelligence Act **CRA** Cyber Resilience Act **CSA** Cybersecurity Act **Cyber Solidarity Act** The EU's proposed law aims to strengthen capacities in the EU to detect, prepare for and respond to significant and large-scale cybersecurity threats and attacks, including through a European Cybersecurity Shield, made of Security Operation Centres interconnected across the EU. **DORA** Digital Operational Resilience Act **NIS2** DIRECTIVE (EU) 2022/2555
United States	**CIRCIA** Cyber Incident Reporting for Critical Infrastructure Act **C-SCRM** The U.S. National Institute of Standards and Technology's (NIST) Cybersecurity Supply Chain Risk Management (C-SCRM) program **CSF 2.0** The U.S. National Institute of Standards and Technology's (NIST) Cybersecurity Framework 2.0 **Cybersecurity Performance Goals** The U.S. Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Performance Goals **EO 14100** Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence **SEC rules** U.S. Security Exchange Commission's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rules
Canada	**AIDA** Artificial Intelligence and Data Act **Bill C-26** New draft critical infrastructure cybersecurity law.
Singapore	**CSA** (Singapore) Cybersecurity Act

About nccgroup

People powered, tech-enabled cyber security

NCC Group is a global cyber and software resilience business, operating across multiple sectors and geographies.

We're a research-led organization, recognized for our technical depth and breadth; combining insight, innovation, and intelligence to create maximum value for our customers.

As society's dependence on connectivity and the associated technologies increases, we help organizations to assess, develop and manage their cyber resilience posture to confidently take advantage of the opportunities that sustain their business growth. With circa 2,200 colleagues, we have a significant market presence in the UK, Europe and North America, and a growing footprint in Asia Pacific.

Service-related certifications and accreditations

- (UK) NCSC Check – we are listed as a green service provider – the highest attainable standard, having held this since 2001.
- ISO 17025:2017 – our NCC Group Security Services Limited entity is certified to this international standard for performing laboratory activities and testing.
- PCI Approved Scan Vendors and PCI Qualified Security Assessor.
- (UK) NCSC Cyber Incident Response – both a Level 1 and Level 2 provider.
- CREST Council of Registered Ethical Security Providers.
- TISAX (Trusted Information Security Assessment Exchange) accredited and awarded a security label to perform automotive security assessments for the German car manufacturing industry.
- FedRAMP – Recognised Third Party Assessment Organization (3PAO) able to offer consultancy and support for clients to become FedRAMP certified.

FOX IT
part of nccgroup

We are here for you

Our experts are here to help you every step of the way. Contact us today to learn more about Global Cyber Security Regulations.

UK & EUROPE +44 (0) 161 209 5200	NETHERLANDS – FOX IT +31 (0)15 284 79 99	NORTH AMERICA +1 (800) 813 3523	AUSTRALIA +61 (0) 2 9552 4451	SINGAPORE +65 6800 0950

Under attack?

Call our 24/7 Incident Response Hotline now

UK & EUROPE +44 331 630 0690	NETHERLANDS – FOX IT 0800-3692378 (NL)	NORTH AMERICA (855) 684-1212	AUSTRALIA 1800 975 310	SINGAPORE +61 2 8379 7870

Disclaimer: This content is for general purposes only and should not be used as a substitute for consultation with professional advisors