IoT Cybersecurity: Regulating the Internet of Things

THALES
Building a future we can all trust

2024 marks a turning point in the evolving landscape of IoT cybersecurity, with significant advancements in laws and regulations in the E.U., the U.S., and the U.K.

The rapid expansion of IoT technology has been matched by an increased focus on securing these devices against cyber threats. This year, significant regulatory milestones have been achieved, shaping how we approach IoT cybersecurity.

This updated web dossier provides a comprehensive overview of the latest E.U., U.S. and U.K. IoT cybersecurity regulatory initiatives.

We will delve into critical guidelines and standards for IoT product security and explore how businesses can stay ahead of regulatory curves.

Remember, while compliance with technical regulations is mandatory, adherence to standards remains voluntary.

Let's explore the latest developments.

Understanding the IoT regulations

Gone are the days when the IoT seemed like an unregulated frontier. Recent years have witnessed the maturation of the IoT regulatory environment, with lawmakers focusing on two primary objectives:

- Enhancing IoT cybersecurity to make connected devices more resilient against cyber threats.
- Safeguarding personal information privacy within the IoT realm.

Different regulatory frameworks govern various aspects of IoT deployment, from data creation to infrastructure and business operations.

Region	Consumer Data Privacy	Cybersecurity
E.U.	**The General Data Protection Regulation** (EU GDPR Directive 95/46/E.C.) Effective May 25, 2018, it became law in the E.U. and the U.K.	**The E.U. Cybersecurity Act** Effective June 27 2019, it became law in the European Union and the U.K. **The NIS Directive 2** Each E.U. country will have to pass a law in October 2024. **The Cyber Resilience Act** Promulgated on December 10, 2024.
USA	There is no comprehensive federal law regulating the collection and use of personal information yet. **Specific laws:** • Healthcare: Health Insurance Portability and Accountability Act • Finance: Gramm-Leach-Bliley Act • Government agencies: U.S. Privacy Act of 1974 • Children's Online Privacy Protection Act	**The Cyber Trust Mark** A voluntary cybersecurtiy labeling program for wireless consumer iot products created by the FCC, to enhance IoT cybersecurity, relying on public private collaboration.
California	**The California Consumer Privacy Act** SB-1121 became effective on January 1 2020 **The California Privacy Rights Act** CPRA took effect on July 1 2023	**The California IoT cybersecurity law** SB-327 became effective on January 1 2020

Most recent regulation frameworks impacting the IoT in Europe and the United States (January 2024)

"The European Union's cybersecurity approach could significantly transform the landscape for IoT product design, redefine business models, and revolutionise the distribution channels across the continent."

Let's see what the Cybersecurity ACT and the Cyber Resilience Act are changing in Europe.

The E.U.'s Cybersecurity Act and Cyber Resilience Act (IoT device security)

The European Union's Cybersecurity Act and the proposed Cyber Resilience Act are two distinct legislative frameworks focused on enhancing cybersecurity and digital resilience across the E.U.

In summary, while both acts aim to enhance cybersecurity in the E.U., the Cybersecurity Act primarily focuses on establishing a certification framework and strengthening ENISA. In contrast, the Cyber Resilience Act introduces specific obligations for products with digital elements, aiming to embed cybersecurity into their entire lifecycle.

Here are the key differences between them:

PURPOSE AND SCOPE

Cybersecurity Act: The Cybersecurity Act (Regulation (E.U.) 2019/881 of April 17 2019) came into force on June 27 2019, and became law in the E.U. and the U.K. It primarily focuses on strengthening the E.U.'s cybersecurity framework. It establishes a permanent mandate for the E.U. Cybersecurity Agency (ENISA) and introduces an EU-wide cybersecurity certification framework for digital products, services, and processes.

Cyber Resilience Act: Proposed in 2022 (Regulation (E.U.) 2024/2847 of October 23 2024), this came into force on December 10 2024 aims to ensure a high common level of cybersecurity across the E.U. It focuses on products with digital elements and seeks to improve their security throughout their lifecycle. This includes everything from design and development to maintenance and disposal.

TARGET

Cybersecurity Act: Targets a broader range of digital products and services, focusing on critical infrastructure and essential services.

Cyber Resilience Act: Specifically targets products with digital elements, including software, hardware, and IoT devices, aiming to address cybersecurity from the design phase.

CERTIFICATION FRAMEWORK

Cybersecurity Act: Introduces a framework for voluntary cybersecurity certification schemes, allowing companies to certify their ICT products, services, and processes according to E.U. standards.

Cyber Resilience Act Goes a step further by proposing mandatory requirements for manufacturers and providers of products with digital elements to ensure compliance with cybersecurity standards from the outset.

REGULATORY OVERSIGHT

Cybersecurity Act: Enhances the role of ENISA, providing it with more resources and responsibilities to support Member States, E.U. institutions, and businesses in cybersecurity matters.

Cyber Resilience Act: Introduces specific obligations for manufacturers, distributors, and importers, including reporting vulnerabilities and incidents, ensuring software updates, and compliance with essential requirements.

IMPACT AND ENFORCEMENT

Cybersecurity Act Focuses on voluntary certification and strengthening national and EU-level cybersecurity capabilities. Initially, manufacturers and vendors will be able to have their products and services meet the E.U. cybersecurity pending standards voluntarily. The certification may eventually be compulsory.

Compliant IoT devices will undoubtedly be labelled. Consumers and businesses may favour these compliant products and services in the long run.

Cyber Resilience Act: Proposes legal obligations with significant penalties for non-compliance, potentially creating a more rigorous enforcement environment.

A landmark development in 2024 is the E.U. Cyber Resilience Act. This regulation imposes stringent EU-wide cybersecurity requirements on digital products, including IoT devices, from design to market availability. It represents a significant step towards standardising IoT device security across the E.U.

The result?

The initial implementation of the Cybersecurity Act strengthens continent institutions. Still, the day-to-day impact will be seen when ICT manufacturers and service providers must be certified for cybersecurity compliance to sell their products.

Like GDPR, these Acts provide a model that other non-EU countries and territories follow when crafting legislation, so getting prepared now will be a competitive advantage for the future.

The General Data Protection Regulation (IoT privacy)

Much has been written on the General Data Protection Regulation, and its impacts are measured worldwide.

The EU GDPR (Directive 95/46/E.C.) establishes a harmonised framework within the European Union and the U.K., the right to be forgotten, unambiguous and affirmative consent and, in particular, severe penalties for failure to comply with these rules.

As of May 25, 2018, only one set of rules directly applies to all European Member States concerning personal data protection.

In summary, the same law applies to 500 million people.

The NIS and NIS 2 Directives (IoT infrastructure)

NIS 1 (MAY 2018)

The Directive on Security of Network and Information Systems (E.U. 2016/1148), or NIS Directive, became applicable on May 24 2018, in the E.U. and the U.K.

This legislative framework aims to reach a high level of cybersecurity for critical national infrastructure and essential services.

The NIS Directive establishes network and information security requirements for operators of essential services and digital service providers, for instance, cloud providers.

- Operators of essential services must identify themselves and link with the applicable Competent Authority – public entities with regulatory and enforcement powers under the NIS Regulations.
- The NIS Regulations also apply to digital service providers, such as online marketplaces, search engines, and cloud computing providers.

How is the NIS Directive different from the GDPR? What's the difference between a Directive and a Regulation?

- The NIS Directive is a legal act and requires the Member States to reach a set of goals. It's up to the Member States to put their laws in the 'spirit' of the NIS Directive.
- The GDRP Regulation has a binding force for all the Member States. It comes from E.U. legislation in its original form and enters into force with no country-by-country variation.

NIS 2 (JANUARY 2023)

The NIS2 Directive broadens the scope of the original NIS Directive by including more sectors and types of entities, thereby expanding the range of businesses that need to comply with stricter cybersecurity rules. Member States have until October 17 2024, to transpose their measures into national law.

While the original NIS Directive allowed member states to adopt different security and incident reporting requirements, the NIS2 Directive aims to harmonise these measures, reducing discrepancies between countries and ensuring a high common level of cybersecurity across all member states.

NIS2 introduces mandatory cybersecurity requirements for a broader range of sectors, including essential entities that comply with stringent cybersecurity rules. This change emphasises a more uniform compliance framework within the E.U.

NIS2 creates the necessary structures and processes for cyber crisis management, reflecting a more proactive and coordinated EU-wide approach to managing cyber threats and incidents.

NIS2 is considered the biggest development in E.U. cybersecurity regulation since the General Data Protection Regulation (GDPR), highlighting its significance in the regulatory landscape and its impact on businesses within the E.U.

The situation is radically different in the U.S. Let's explain.

IoT regulations in the U.S. (Cybersecurity Improvement Act)

There's no national IoT cybersecurity regulatory framework nor a comprehensive set of standards as of March 2025 in the U.S.

In March 2019, the 2019 IoT Cybersecurity Improvement Act was introduced by members of the U.S. Senate (S.734) and House of Representatives (H.R. 1668).

The bill passed on December 4 2020, sets minimum security standards for connected devices the federal government uses.

The authors avoid directly regulating the private sector, potentially slowing innovation.

Instead, this bipartisan legislation aims to leverage Federal Government procurement influence to encourage increased cybersecurity and put basic security measures for IoT devices.

The bill gives the National Institute of Standards and Technology (NIST) the authority to oversee IoT cybersecurity risks for equipment bought by the federal government.

Specifically, the text mandates NIST to issue security development, identity management, upgrade, and configuration management guidelines for IoT products.

It requires that any purchase by the federal government comply with these recommendations. Manufacturers not adopting these guidelines would be turned down by the vast federal government markets.

The bill also calls upon IoT device manufacturers to adopt coordinated disclosure policies.

In other words, the information is swiftly shared if a vulnerability is found.

> "Under the IoT Cybersecurity Improvement Act of 2020, federal agencies are barred from acquiring or utilising IoT devices deemed "non-compliant" with the cybersecurity standards set forth by NIST beyond the date of December 4, 2022."

THE CYBER TRUST MARK

The Cyber Trust Mark program is an initiative launched in the United States in 2023 aimed at enhancing cybersecurity for consumer devices. This program introduces a labeling system for Internet of Things (IoT) devices to indicate that they meet certain cybersecurity standards set by the government. The Cyber Trust Mark is intended to help consumers make informed choices about the security of the products they purchase and to encourage manufacturers to follow best practices in cybersecurity. This approach seeks to mitigate the risks associated with using interconnected devices by ensuring they adhere to robust security measures.

HOW IS EXECUTIVE ORDER 14028 RELATED TO IOT?

Executive Order 14028, signed on May 12, 2021, is directly related to the security of the Internet of Things (IoT) in several ways:

- Setting Security Standards: The order mandates the establishment of minimum security standards for IoT devices owned and operated by the federal government, ensuring that these devices are protected against cyber threats.
- Cybersecurity Labeling for Consumers: Part of the order includes developing a labelling program for IoT devices to inform consumers about the security features of these products, similar to energy efficiency labels on appliances.
- Agency Responsibilities: The order requires agencies to enhance their cybersecurity, which includes the security of IoT devices within their software supply chains, making it a priority for federal procurement and operations.
- Zero Trust Architecture: Agencies are encouraged to adopt zero trust principles, particularly relevant to the secure deployment and management of IoT devices within government networks.

This Executive Order represents a concerted effort to safeguard IoT infrastructure as part of the broader initiative to improve the nation's cybersecurity posture.

CALIFORNIA'S AND OREGON'S IOT CYBERSECURITY LAWS (IOT SECURITY)

California legislature passed a new IoT security law in 2018 that became effective on January 1 2020 (in addition to the CCPA we will see later).

Just think about it.

This was the first IoT-specific security law in the country.

California's SB 327 defines new security requirements for IoT devices connected directly or indirectly to the Internet with an I.P. or Bluetooth address. These devices sold in California must be fitted with "reasonable security features."

Its goal is to better address the risks that increased levels of connectivity could bring.

The security features should protect the IoT device and its data. In particular, if the device integrates a password, it must either be uniquely linked to that device or require the user to set their password during the initial setup.

The case settled in July 2019 against D-Link Systems by the Federal Trade Commission illustrates the basic levels of security that the law now mandates.

Contrary to D-Link's claims that its routers and I.P. cameras were protected by "advanced network security," the FTC discovered that the company used hard-coded passwords that clients could not change. The devices also stored user credentials in plain text, a windfall for a straightforward password-guessing cyber-attack.

Today, "reasonable secure features" are no longer an option in California. IoT devices will be less risky since they will no longer work with a manufacturer's "generic" default password.

The definition of a "reasonable security feature" is vague and lacks detailed instructions that IoT manufacturers need.

However, California's IoT law is a significant first step as it targets IoT devices and basic cyber-attack methods that can leave consumers vulnerable to security and privacy risks.

There's more.

SB-327 places liability (and burden of proof) on the IoT vendors if the device is connected to the Internet in California.

Oregon (HB-2395) joined California with a similar text that went into effect on January 1, 2020.

Data privacy federal framework (IoT privacy)

As of January 2024, the country has no "GDPR-like," comprehensive federal law regulating the collection and use of personal information.

Instead, according to Thomson Reuters' practical law, it has a patchwork combination of federal and state laws and regulations that sometimes overlap or contradict one another.

By contrast, some industry sectors and their related markets are restricted by specific U.S. laws. Vendors unable to meet these restrictions are effectively locked out of these highly profitable contracts.

In particular, the healthcare technology industry has its requirements in the United States, as defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Federal Exchange Data Breach Notification Act of 2015.

- HIPAA specifies national standards for the privacy and protection of healthcare information.
- The latter formalises strict rules on notifying individuals when their health insurance information has been compromised.

This means that devices that may have access to that information, including the connected medical devices (aka the Internet of Medical Things - IoMT), must protect their data and report if their security is breached.

Another primary legislation from the 90s, the Gramm-Leach-Bliley Act (GLBA), is a banking and financial law with crucial data privacy and security requirements.

Privacy laws in the U.S. States (IoT privacy)

As of December 2023, 12 states have such legislation – California, Virginia, Connecticut, Colorado, Utah, Iowa, Indiana, Tennessee, Oregon, Montana, Texas, and Delaware, according to the Blomberg Law website.

The California Consumer Privacy Act (SB-1121) became effective on January 1, 2020, and applies to companies operating in California.

The bill enhances privacy rights and consumer protection for residents of the Golden State. In November 2020, Californian voters made another step forward on the data privacy route.

The California Privacy Rights Act (CPRA), passed into law on November 3 2020, took effect on January 1 2023, with a lookback period from January 1 2022.

It's a supplement to CCPA. It creates a series of new amendments to the existing text. In particular, it creates new rights and expands existing ones for California residents.

CRPA creates a new category of personal information named sensitive personal information. Biometric data, along with race, ethnicity, sexual orientation, religious beliefs, and geolocation or social security number, to name a few, are included in this new group.

New York State now stands beside California with its SHIELD Act.

The data security and privacy provisions of New York's Stop Hacks and Improve Electronic Data Security Act («SHIELD Act» State bill S55575B) went into effect on March 21 2020. The bill requires a cybersecurity program and protective measures for N.Y. State residents.

These are new laws that IoT manufacturers should take into account.

U.K.: Are you ready for April 2024?

The U.K. has established mandatory cybersecurity laws and regulations for Internet of Things (IoT) devices, came into effect on April 29, 2024.

This legislation, known as the Product Security and Telecommunications Infrastructure (PSTI) Act, impacts businesses involved with consumer IoT products. It's shifting the responsibility away from consumers to secure their own devices by ensuring strong cybersecurity is built into these products by design.

The regulations require compliance with new product safety requirements for connected products, encompassing a broad range of consumer connectable devices including, but not limited to, connected safety-relevant products such as door locks and home automation devices.

These regulations aim to enhance the security and safety of IoT devices in response to the growing concerns about cybersecurity in the digital age.

The legislation for IoT devices focuses on three crucial areas of compliance that significantly impact the fire and security market:

Clear Information on Support Period at Point of Sale: Manufacturers must provide explicit information about the duration they will offer updates and support for their

products. This transparency ensures that consumers know the timeframe of support they can expect for their IoT devices.

No Default Passwords: The law mandates that each product have a unique password, which must be used at first login. This password cannot be reused, ensuring each device is secured with a distinct and robust password from the outset. This requirement addresses the common security risk of devices having easily guessable or common default passwords.

Reporting of Security Issues: Manufacturers must establish and communicate clear procedures for reporting security vulnerabilities. This includes providing contact information for reporting vulnerabilities and ensuring that customers are promptly informed about any identified vulnerabilities and provided with timely fixes. This aspect of the law emphasises the importance of active management of security risks and the need for ongoing vigilance in IoT security.

The recently enacted legislation formalises cybersecurity protocols that, until now, were implemented voluntarily within the U.K.

This move by the U.K. aligns closely with the E.U.'s Cyber Resilience Act, creating a comparable framework for cybersecurity standards, as analysed by Bird &Bird.

Cybersecurity IoT guidelines and standards

Various policies, standards, best practices, and guidelines are available from different sources.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

In the U.S., for example, the National Institute of Standards and Technology (NIST) released in February 2022 a white paper on "Recommended criteria for cybersecurity labelling in the IoT."

They are designed to help IoT manufacturers and integrators in all sectors develop securely. The organisation stresses that the guidelines are voluntary and focus on six simple features that consumers should look for:

- A unique identifier (a serial number, for instance)
- The ability to change firmware configuration
- Data Protection
- Secure access to administrative control
- The ability to update firmware and software
- Cybersecurity event logging

Needless to say, it's essential reading.

INTERNATIONAL ORGANIZATION FOR STANDARDS

At the highest international level, the International Organization for Standards has released five standards to cover all aspects of cybersecurity.

These documents are broad in scope, with IoT as an inherent part of these standards.

- **ISO/IEC 27001** (best-practice information security management systems)
- **ISO/IEC 27032** (cybersecurity)
- **ISO/IEC 27035** (incident management)
- **ISO/IEC 27031** (readiness for business continuity)
- **ISO/IEC 22301** (business continuity management systems)

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA)

ENISA is actively contributing to European cybersecurity policy, as we mentioned earlier.

The Athens-based organisation recently published "Good Practices for Security of IoT - Secure Software Development Lifecycle" (November 2019). This guide details how to implement security by design for IoT in addition to its 2017 publication «Baseline Security Recommendations for IoT Security.»

INDUSTRY ASSOCIATIONS AND CONSORTIA

Consortia and industry associations also shape the IoT ecosystem with agreements to ensure standardisation for compatibility, secure interoperability, safety, and quality.

Notably, the CTIA (CTIA - The Wireless Association), representing the U.S. wireless communications industry and companies throughout the mobile ecosystem, is going one step further.

The nonprofit organisation operates six device certification programs for IoT devices, from battery quality and hardware reliability to IoT cybersecurity.

The cybersecurity certification process, in particular, includes verifying the device's security features against cybersecurity best practices for storing consumers' information, password and security management standards, and over-the-air mechanisms for software updates.

Regulating the Internet of Things: the future

Self-regulatory regimes inspired (or not) by safety standards are gradually replaced by country-specific regulations imposing security implementation requirements.

Based only on the current legal requirements, the minimum level of requested cybersecurity for vendors and manufacturers is attainable.

However, the first step is regulatory compliance on basic security for individual IoT devices.

Network operators need to take additional actions. They can implement more high-level cyber-security and solutions that go beyond the performance of individual devices to address the IoT more holistically and comprehensively.

More resources on cybersecurity IoT standards and recommendations

- Australia's Code of Practice for Securing the Internet of Things for Consumers
- The UK Code of Practice for Consumer IoT Security
- The UAE IoT framework from the PWC website
- Cybersecurity laws and regulations in India (2024)
- GSMA IoT Security Guidelines
- Center for Internet Security: Cybersecurity best practices
- FCC regulations (Federal Communications Commission)
- The CE marking and IoT products
- The Federal Financial Institutions Examination Council (FFIEC)

THALES

Building a future we can all trust

thalesgroup.com