

Publication date:

May 2025

Author:

Hollie Hennessy

Consumer IoT Device Cybersecurity Standards, Policies, and Certification Schemes 2025



OMDIA

Omdia commissioned research, sponsored by Connectivity Standards Alliance

Contents

Summary	2
Part 1: Consumer IoT security regulations	3
Part 2: Voice of the consumer	42
Conclusion: Time for reliably secure IoT products	50
Appendix	51

Summary

At the core of Internet of Things (IoT) cybersecurity are three key elements: standards, regulations, and labels. Standards are created to harmonize a common set of requirements. Regulations are implemented to drive manufacturers toward adopting robust cybersecurity practices, safeguarding societies, and enhancing overall cyber resilience. Labels are created to provide visibility to consumers.

Labels and regulations rely on standards to harmonize applicability. Labels can be a product of regulations or of industry-driven initiatives. Therefore, there is a combination of both interrelation and independence if they are created in isolation. This is one of the factors that has resulted in a fragmentation of IoT cybersecurity requirements worldwide.

Omdia has published this research report, sponsored by the Connectivity Standards Alliance (the Alliance), to provide some context on emerging trends in IoT cybersecurity. Because events are rapidly unfolding in this area, the statements in this document should be taken as a snapshot in time and a best-effort summary of the current situation. Nevertheless, they provide a clear and compelling portrait demonstrating the importance of IoT cybersecurity and the strong demand for cybersecurity certifications in this area.

In response to this need, the Alliance is developing an IoT product cybersecurity certification program that will aim to meet the demands of consumers and governments while keeping the process for product makers manageable. This report covers the landscape for consumer IoT device security standards, policies, and national certification schemes. The Alliance product security certification program details are not included.

Part 1: Consumer IoT security regulations

Growing need for IoT cybersecurity standardization and labeling

Standards and labeling requirements are being proposed for IoT devices with the lead being taken by the European Telecommunications Standards Institute (ETSI), the National Institute of Standards and Technology (NIST) in the US, and the International Organization for Standardization / International Electrotechnical Commission (ISO/IEC). In addition, CEN, the European Committee for Standardization, and CENELEC, the European Committee for Electrotechnical Standardization, along with ETSI, make up the three European Standardization Organizations officially recognized by the EU and the European Free Trade Association (EFTA) to officially develop and define voluntary standards at an European level.

Despite best efforts to increase harmonization through standardization, IoT cybersecurity standards continue to be disparate. This has resulted in a fragmented picture globally with different regions taking multiple approaches and a lack of unification.

Although the IoT cybersecurity standardization landscape is only emerging, connected consumer devices are already proliferating in homes globally. Omdia is forecasting high growth in the adoption of smart home IoT devices, which include examples such as:

- Consumer electronics (home audio, health/fitness, and appliances)
- Lighting and control devices (lighting, plugs/switches, and blinds/shades)
- Safety and security devices (cameras, electronic locks, intruder alarms, video doorbells, garage door operators, hazard detectors, and smart speakers)
- Climate control (air conditioners, thermostats, radiator valves, and fans)

Associated products and services through which these devices connect include: routers, gateways, smartphones/tablets, mobile applications, and the cloud services that connect them.

The security of IoT devices is of concern for several reasons. First, many IoT devices connect to the internet. Paired with this, historically there have been several IoT security vulnerabilities that need to be addressed. IoT devices, especially consumer devices, are often vulnerable for a few reasons

such as hardware or software vulnerabilities. The proliferation of devices poses a real risk, especially when it is combined with a rapidly evolving threat landscape. With this connectivity and potential vulnerabilities, attackers could reach millions of homes, putting devices in jeopardy for use as botnets, for example, by bad actors in wider attacks.

An example of this, and something which spurred the IoT cybersecurity market, regulation and attention, was the large-scale Mirai botnet, which was discovered in 2016. The distributed denial of service (DDoS) attack infected hundreds of thousands of devices, bringing down a number of websites from X (formerly Twitter) to Airbnb.

IoT is a fast-moving market, and Omdia forecasts that by 2026 there will be around 52.2 billion installed devices. With this level of growth, the impact of a similar incident will likely be exacerbated by the massive attack surface that these devices represent.

The COVID-19 pandemic drove an increase in the use of connected products and introduced new ways of living and working enabled by technology. Many use cases provide greater value and convenience for consumers. This trend is expected to continue with connected technology and new value-added services in areas such as transportation, energy management, and healthcare. Again, with this increased use of technology in people's daily lives, the potential threat vectors available for criminals will increase.

Most countries around the world are concerned with protecting their citizens against these growing threats and are asking a number of questions, summarized in **Figure 1**, to address these issues.

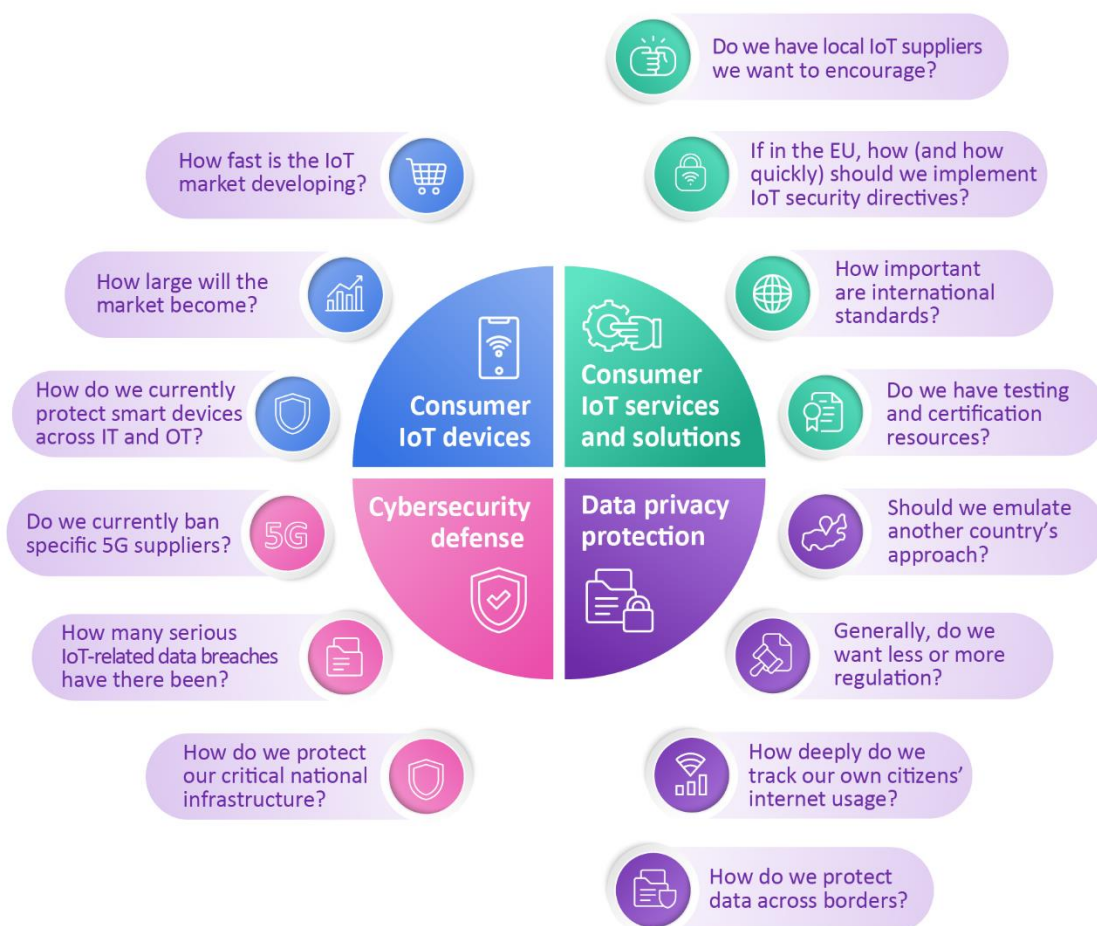
In response, national, regional, and international organizations for standards are providing recommendations and guidance to governments and private organizations to help them improve the security of consumer IoT products and services. In particular,

- ETSI published its EN 303 645 standard, "Cybersecurity for Consumer Internet of Things: Baseline Requirements 2.1.1," in June 2020. ETSI is Europe based and has been the fastest of the three main organizations listed here to address IoT security. This is currently the most widely used and referenced standard in this area. The standard was most recently updated in 2024 to 3.1.1.
- In the US, NIST published its "Profile of the IoT Core Baseline for Consumer IoT Products" in September 2022, part of the organization's response to White House Executive Order 14028 in 2021. The profile was developed out of a NIST white paper: "Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products," also published in 2022.
- Also relevant is the work of ISO/IEC, an international, non-governmental organization. Although there is currently less adoption, it has published several standards including ISO/IEC 27402:2023, "Cybersecurity — IoT security and privacy — Device baseline requirements." The first edition was published in 2023.

The above organizations and others in the field are working independently to further develop their standards for IoT device security. This, coupled with each country's own perspective, local experiences, and regulatory requirements, is resulting in an increasingly fragmented landscape

where understanding which standards apply is becoming more complex by market, country, and region.

Figure 1: Typical questions being asked about IoT security by national governments



© 2025 Omdia

Source: Omdia

Implementations of standards vary significantly by country, but what follows is a broad overview of the three baseline standards and organizations noted above.

NIST: Addressing products and developers

The National Institute of Standards and Technology (NIST) is part of the US government under the Department of Commerce. It is a nonregulatory body, focused on innovation and industrial competitiveness by way of science, standards, and technology. It has been active in addressing the need for consumer IoT security, especially since then-president Joe Biden's executive order (EO) on "Improving the Nation's Cybersecurity (14028)" was issued in May 2021. This EO called on NIST to:

- Publish guidance referencing "standards, procedures, and criteria"
- Initiate two security-labeling programs related to IoT and software

Regarding IoT cybersecurity, NIST has published the NIST IR 8259 series of reports, which include:

- "Foundational Cybersecurity Activities for IoT Device Manufacturers," looking at how manufacturers can approach cybersecurity for IoT in general (IR 8259)
- "IoT Device Cybersecurity Core Baseline" (IR 8259A) and "IoT Non-Technical Supporting Capability Core Baseline" (IR 8259B) defining the core baseline, which manufacturers can use as a starting point

Further, there is also NIST IR 8425 "Profile of the IoT Core Baseline for Consumer IoT Products," published in September 2022. This report sets out multiple capabilities from two angles: IoT product capabilities (satisfied by software and hardware) and IoT product developer activities (satisfied through actions and evidence) drawn from the IR 8259 series. The profile defined in this report also draws on threats specific to consumer IoT, with mapping to the MITRE ATT&CK framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. Overall, NIST has taken a broad view, looking at an IoT product as a whole, including backend and mobile apps as well as device level, in its scope.

In addition to these reports, NIST has published essays, profiles, and other documents and runs workshops on IoT cybersecurity.

In July 2023, the White House announced its plans for the Cybersecurity Labeling Program for Smart Devices to Protect American Consumers, known as the "Cyber Trust Mark"—including participation from the Federal Communications Commission (FCC) and the Departments of Energy and State, as well as NIST. NIST was directed to "immediately undertake an effort to define cybersecurity requirements for consumer-grade routes", given one of the most at risk and thus prioritized device type.

Since then, NIST has published several publications to support the task, including:

- Crosswalk of Consumer-Grade Router Cybersecurity Standards to NIST's Baseline for Consumer IoT Products, in October 2023

-
- Initial preliminary and second preliminary drafts of the Recommended Cybersecurity Requirements for Consumer-Grade Router Products in November 2023 and February 2024, respectively
 - NIST IR 8425A: Recommended Cybersecurity Requirements for Consumer-Grade Router Products, in April 2024

In March 2024, the FCC adopted rules for the IoT Cybersecurity Labeling Program for wireless consumer IoT products, creating the voluntary cybersecurity labeling program; “U.S. Cyber Trust Mark,” discussed in more detail below. On January 7, 2025, the FCC and the White House launched the program.

ETSI: Standards for IoT device cybersecurity

The European Telecommunications Standards Institute (ETSI), a European standards organization, is one of the recognized standards development organizations (SDO) in Europe, alongside CEN and CENELEC. Its role in Europe is to support European regulation and legislation through the development of harmonized European standards. That said, the organization has a global perspective and impact. It has 900 members from more than 60 countries, many of which are outside the EU. In addition to its activities related to consumer IoT security, ETSI is also involved in developing standards for areas as varied as edge computing, low-throughput networks, and next-generation protocols.

ETSI EN 303 645, initially released in June 2020, was the first globally applicable standard for consumer IoT products. The standard was developed from technical specifications drafted by TC CYBER (an ETSI technical committee), released in February 2019, and from the UK government’s Code of Practice for Consumer IoT Security, first published in March 2018. The fact that the first globally used standard was released so recently is reflective of how rapidly the IoT market is developing and how security issues are only recently being addressed in this fast-moving space. This is one of the reasons why the global IoT security regulatory landscape is fragmented.

The current version of ETSI EN 303 645, released in 2024, specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the internet or home network) and their interactions with “associated services.” Associated services are typically defined as digital services that, together with the device, are part of the overall consumer IoT product and are typically required to provide the product’s intended functionality. They can also include mobile applications, cloud computing/storage, and third-party application programming interfaces (APIs). Although these services are referenced throughout the standard, ETSI defines them as out of scope, focusing more on the device. The September 2024 update, 3.1.3, includes additions and further clarity to remove any confusion plus data protection provisions not in the original version. These include reference to ETSI TR 103 838 as an example of a vulnerability disclosure policy, improved guidance for resource-constrained devices, improved guidance surrounding labeling, more details and examples regarding clarity and transparency with data collection, as well as provision 6-6 regarding data storage and processing.

The ETSI EN 303 645 standard is designed to prevent large-scale attacks on smart devices. It establishes a security baseline for connected consumer products and can be used as a basis for future IoT certification schemes. It includes 13 cybersecurity recommendations, where the top 3 are: 1) no default passwords, 2) implement a vulnerability disclosure policy, and 3) keep software updated. These three requirements are often focused on by governments and have, in fact, become the key requirements of existing regulation in the UK (the Product Security and Telecommunication Infrastructure Act).

The standard also includes a specific section on six data protection provisions for consumer IoT, intended to be supplemental to General Data Protection Regulation (GDPR) legislation and looking at data protection from a technical angle.

Examples of countries that have adopted ETSI EN 303 645 include

- Finland – national Consumer IoT Certification Scheme
- Singapore – national Cybersecurity Labeling Scheme
- Vietnam – Ministry of Information and Communications

See **Figure 4** for more information.

Numerous testing laboratories and certification bodies such as TÜV (Germany), SafeShark, DEKRA, BSI (Germany), and VDE have adopted this standard for developing proprietary IoT security certification labels.

Figure 2: ETSI's suite of IoT security guidelines

Requirements specifications	Description
EN 303 645 TS 103 645	All consumer IoT devices; provides baseline requirements
Assessment specification – TS 103 701	Baseline conformance assessment; self assessment (first party) and independent evaluators (third party)
Implementation guide – TS 103 621	Implementation guidance with use case examples
Vertical standards / domain-specific extensions	Prescriptive, testable, and stringent specifications using EN 303 645 as a baseline

© 2025 Omdia

Source: ETSI and Omdia

ETSI has also published the ETSI TS 103 701 assessment specification, which includes mandatory and recommended tests for associated laboratories and manufacturers, and the ETSI TR 103 621 implementation guide. ETSI's TC CYBER group is also working on specific templates or profiles applicable to vertical sectors such as smart locks, mobile devices, and gateways, among others.

ISO/IEC: Device trustworthiness

Also noteworthy is the related work of the International Organization for Standardization (ISO), which publishes standards in all fields apart from electrical and electronic engineering—the responsibility of the International Electrotechnical Commission (IEC).

ISO and IEC form a connected nongovernmental standards organization. They have jointly taken up responsibility for drawing up ICT standards. ISO IEC JTC1 SC27 is the technical subcommittee tasked with the development of standards on information security, cybersecurity, and privacy protection. Comparable to NIST and ETSI standards detailed above, it has a draft standard focused on baseline requirements for IoT devices, part of the ISO27k family of standards, which all focus on managing information risks by implementing security controls. This is ISO/IEC 27402 “Cybersecurity — IoT security and privacy — Device baseline requirements,” which is the most recently published of the major standards, in November 2023.

ISO/IEC 27402 builds on and supports the security controls documented in the published ISO/IEC 27400 “Cybersecurity — IoT security and privacy — Guidelines” (2022). Another notable publication

is ISO/IEC 27403:2024 “Cybersecurity — IoT security and privacy — Guidelines for IoT-domotics,” aimed at the designers, manufacturers, and security assessors of IoT domotics (home automation), published in June 2024.

The SC27 subcommittee is also working on a framework and methodology for implementing and maintaining the trustworthiness of IoT systems and services and doing work on the ISO/IEC 27404 labeling scheme for labeling for consumer IoT devices, which is currently in the enquiry stage with ISO members.

ISO is headquartered in Geneva, Switzerland. As a global standards organization, it relies on contributions from 167 member countries.

The commonality of standards and schemes

All three major standards bodies—NIST, ETSI, and ISO/IEC—have established baselines for consumer IoT device security. They are also gradually making progress toward labeling schemes. Over time, we expect to see some crossover in their approaches in formal and informal ways. For example, NIST calls out conformity and lists ETSI EN 303 645 as an example standard used for conformity. However, as we have seen in other areas of the industry, when it comes to standardization it can take a long time before harmonization is achieved across verticals, geographies, and industries. A current high-level comparison of the key standards is shown in **Figure 3**.

Figure 3: Comparison of key standards

Standard	Test specification	Label guidance	Summary
ETSI EN 303 645	ETSI TS 103 701	No	• Very prescriptive and primarily focused on functional testing with some documentation requirements • Has a fully defined test specification • Will produce derivative test specs for various IoT device categories
NIST IR 8425	No	Yes	• Broader with more focus on documentation/SDL • Leaves open how to test against the requirements • NIST calls out conformity and lists EN 303 645 as an example standard used for conformity • More opinionated on what a label will look like
ISO 27402	No	Yes – 27404	• High-level set of more generic requirements

© 2025 Omdia

Source: Omdia

The implementation of standards from NIST, ETSI, and ISO/IEC varies significantly by geographic region. A few countries have introduced certification and/or labeling schemes, most on a voluntary rather than compulsory basis. Others have committed to certification and/or labeling schemes but are still in the development phases. However, 9 of the 14 countries examined for this study have referenced ETSI EN 303 645. Countries were chosen based on whether there was government activity around consumer IoT device specifications.

Figure 4: Summary of IoT device security specifications by geographic region

Region	IoT device security specification	Mandatory/voluntary	Certification/statement of compliance	Labeling	Key standard referenced
Asia & Oceania					
Australia	Yes	Mandatory*	Yes	Yes	ETSI EN 303 645
China	Yes	Mandatory	Yes	No	ISO/IEC 27403:2024
India	Yes	Voluntary and mandatory	Yes	Yes	ETSI EN 303 645, ETSI TS 103 701, OWASP ASVS, ISVS, ISO/IEC 27402
Japan	Yes	Voluntary	Yes	Yes	NIST, ETSI EN 303 645, IEC 62443 -4 -1, NIST IR 8425, ISO/IEC 27404
Singapore	Yes	Voluntary	Yes	Yes	ETSI EN 303 645
South Korea	Yes	Voluntary	Yes	Yes	ITU X.1352
Taiwan	Yes	Voluntary	Yes	Yes	ETSI, MTFSB, national standards
Thailand	Under development	Voluntary	No	No	None
Vietnam	Yes	Voluntary	No	No	ETSI EN 303 645
Europe					
Finland	Yes	Voluntary	Yes	Yes	ETSI EN 303 645
France	Yes	Voluntary	No	No	ETSI EN 303 645
Germany	Yes	Voluntary	Yes	Yes	ETSI EN 303 645
Spain	No	Voluntary	No	No	None
UK	Yes	Mandatory	Yes	Yes	ETSI EN 303 645
Americas					
Brazil	Yes	Mandatory	Yes	Yes	ETSI EN 303 645, ISO/IEC 27402
US	Yes	Voluntary	Yes	Yes	NIST IR 8425

Notes: *Will be mandatory.

© 2025 Omdia

Source: Omdia

Global summary and findings by region and country

Asia & Oceania

Australia

The Australian government is an early adopter of IoT security standards. In October 2020, the Department of Home Affairs introduced its code of practice “Securing the Internet of Things for Consumers” based on compliance with the 13 principles set out in ETSI EN 303 645. It considers the first three principles as the most important:

- No duplicated default or weak passwords
- Implement a vulnerability disclosure policy
- Keep software securely updated

The code of practice covers “everyday smart devices that connect to the Internet – such as smart TVs and home assistants ...,” because “these devices are developed with functionality as a priority, and security features are often absent or an afterthought.” It covers consumer-grade internet-connected devices and associated applications (e.g., wearable devices and home appliances such as smart TVs and refrigerators). The guidelines do not include mobile phones, which are covered by other guidance.

The Behavioural Economics Team of the Australian Government (BETA) has tested IoT product labeling with 6,000 consumers online, proposing three types of labeling, of which the “graded shield” proved most popular.

Figure 5: Proposed options for Australian IoT device security labeling

Text Expiry	Icon Expiry	Graded Shield
Security updates guaranteed until June 2021	 SECURITY UPDATES GUARANTEED UNTIL JUNE 2021 cybersecurity.gov.au	CYBER SECURITY RATING BASELINE  cybersecurity.gov.au
Security updates guaranteed until February 2022	 SECURITY UPDATES GUARANTEED UNTIL FEB 2022 cybersecurity.gov.au	CYBER SECURITY RATING INTERMEDIATE  cybersecurity.gov.au
Security updates guaranteed until August 2023	 SECURITY UPDATES GUARANTEED UNTIL AUG 2023 cybersecurity.gov.au	CYBER SECURITY RATING ENHANCED  cybersecurity.gov.au
Security updates guaranteed until August 2026	 SECURITY UPDATES GUARANTEED UNTIL AUG 2026 cybersecurity.gov.au	CYBER SECURITY RATING HARDENED  cybersecurity.gov.au

Source: Australia Department of Home Affairs

This labeling approach is being developed alongside regulation; Australia believes it is the first country to do this. However, it has decided against introducing a mandatory label. As part of its

2023-2030 Cyber Security Strategy, the government announced it would develop a voluntary labelling scheme for consumer-grade smart devices.

Although the Code of Practice is voluntary, the Australian government's Cyber Security Act 2024 was signed into law on November 29, 2024, with regulation coming into force 12 months after receiving Royal Assent. The Cyber Security Act includes measures to:

- Mandate minimum cybersecurity standards for smart devices (Part 2 of the Cyber Security Act 2024)
- Introduce a mandatory ransomware and cyber extortion reporting obligation for certain businesses
- Encourage industry engagement with government following cybersecurity incidents
- Establish a Cyber Incident Review Board for knowledge sharing and review

Regarding the security standards for smart devices, the act places responsibility on manufacturers and suppliers, requiring a statement of compliance. The act provides the Secretary of Home Affairs the ability to issue enforcement notices, which can extend to recall notices and public notification.

In its approach to privacy and cybersecurity regulations, Australia publicly claims to follow the approach taken by the UK with the Product Security and Telecommunications Infrastructure (Requirements for Relevant Connectable Products) Regulations, based on the first three principles from ETSI EN 303 645.

China

The Chinese Ministry of Industry and Information Technology (MIIT) released its draft guidelines for the construction of basic security standard systems for IoT in January 2021, asking for comments from interested parties, which were eventually published in September 2021. In addition, it has announced the adoption of ISO/IEC 27403:2024.

It introduced the Personal Information Protection Law (PIPL) in February 2022, which states that IoT suppliers must get prior consent from consumers to obtain and process their data, stops them from denying services to those who opt out from having their data used, and introduces strict rules on where and how data is transferred. Heavy fines have been introduced for noncompliance. This was updated in March 2024, easing restrictions on cross-border data transfer.

China also launched a new Data Security Law in September 2022, which included cross-border data transfer regulations, such as the inspection of personal consumer information transferred beyond the Chinese border and the seizure of data deemed to be threatening to national security, the economy, or general public interest.

In addition, the State Council of China officially passed the Network Data Security Management Regulations, which came into force as of January 1, 2025. The regulations apply to those involved in

data processing within China, surrounding the classification of important data and management of data transfers as well as data protection measures.

China recognizes its IoT market's scale and rapid development. As such, it has issued an Implementation Plan for the New Industry Standardization Leading Project (2023-2025), setting goals for 2025, including the creation of more than 30 national and industry standards in the IoT field as well as participation in more than 10 international standards. The Ministry of Industry and Information Technology document "Internet of Things Standardization System Construction Guide (2024)" highlights several security and trust standards including:

- IoT security architecture
- Security classification
- Terminal security
- Transmission security
- Data security
- Platform (system) security
- Security management

The document also references other cybersecurity themes such as data protection, network security, edge computing security and digital twin security.

India

In August 2021, the Indian government in partnership with its Telecommunication Engineering Center introduced a voluntary "Code of Practice for Securing Consumer Internet of Things (IoT)." The approach is based on ETSI TS 103 645 and EN 303 645. There is also an expectation that the ETSI TS 103 701 (cybersecurity assessment for consumer IoT products) standard will help in implementing these guidelines. Unlike in Australia, there is no mention in India of following the UK's approach.

Part of India's motivation comes from its 2018 National Digital Communication Policy (NDCP), which planned for the creation of an ecosystem of 5 billion connected devices by 2022. Mandatory testing and certification of certain IoT devices are already covered by the Indian Telegraph (Amendment) Rules introduced in 2017, and there is a stated need to create a central mechanism, such as a national trust center, for registration of certified devices to address new vulnerabilities as they arise.

The aim of India's approach is to ensure end-to-end security for connected IoT devices, with a second nested aim of protecting the privacy of the personal data of individuals, especially in the healthcare arena.

In 2018, India passed its Personal Data Protection Bill, which mandates that there be clarity in what personal data suppliers process, that data be obtained only through consumers' consent, and that

consumers retain their right to data withdrawal. In applying this to IoT devices, this code of practice suggests that users should expect to preserve their privacy by configuring devices and associated services appropriately and that personal data collected through telemetry by suppliers should be kept to the minimum necessary for the intended function.

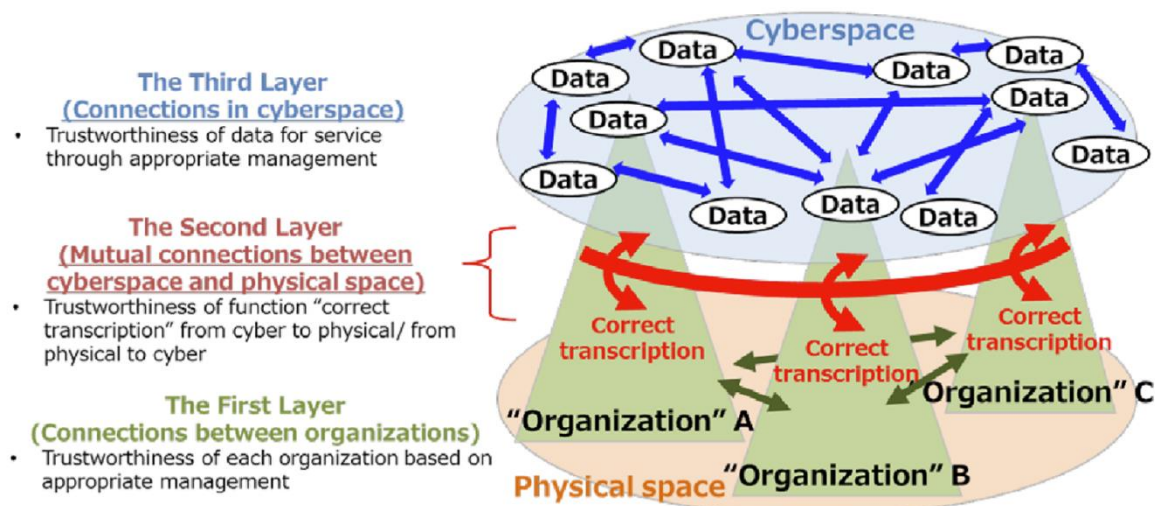
In addition, in December 2023, India released the IoT System Certification Scheme (IoTSCS), which includes evaluation of several components of IoT products and systems including security architecture review, penetration testing, code review, and compliance assessment. It categorizes into three assessment levels:

- Level 0 – minimal assurance, but must seek Level 1–3 certification within a year
- Level 1 – low assurance, minimum requirements that all IoT devices should meet
 - **A baseline security for connected devices**
- Level 2 – for IoT devices that contain sensitive data; recommended for most IoT devices
 - **To provide protection against the attacks that go beyond software and target the hardware of the device**
- Level 3 – for critical IoT devices as well as applications that perform high-value transactions, contain medical data, or require high levels of trust
 - **To provide requirements for devices where compromise should be avoided at all costs**

Japan

Japan's approach to IoT security initially concentrated on enterprise issues of trustworthiness and on the deployment of IoT devices and how they are used, as well as some coverage of IoT security within related mandatory requirements. It has since also developed its IoT Product Security Conformity Assessment Scheme in August 2024.

Figure 6: Japan’s three-layer Cyber/Physical Security Framework (CPSF) model including the trustworthiness in each layer



Source: Japan METI IoT Security Safety Framework

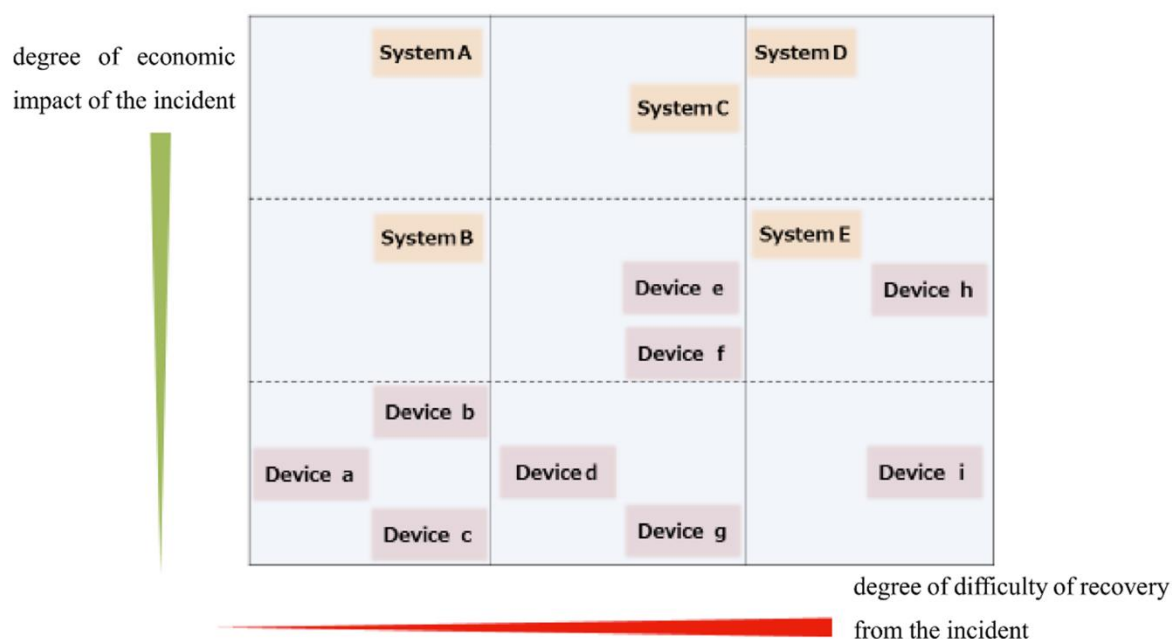
Japan’s Ministry of Economy, Trade and Industry (METI) launched its IoT Security Safety Framework (IoT-SSF) in 2020. It is designed to enable players in different industries to use the same approach for reviewing the security and safety in devices and systems and not to establish mandatory rules uniformly applied to IoT devices and systems irrespective of industry and use. In the framework, IoT devices are described as “new devices for connecting cyberspace and physical space,” which form the connections in Layer 2 of the model (see **Figure 6**).

The IoT-SSF analyzes the impact of device vulnerability on two axes:

- The degree of difficulty of recovery from an incident, listed as limited, serious, and severe damage
- The degree of economic impact of the incident in monetary terms, listed as limited, serious, or catastrophic

It uses these to map the hidden risks of devices and systems into nine segments by organizing them by the three difficulties of recovery and the three economic impacts.

Figure 7: The categorization of devices and systems connecting physical space and cyberspace in Japan



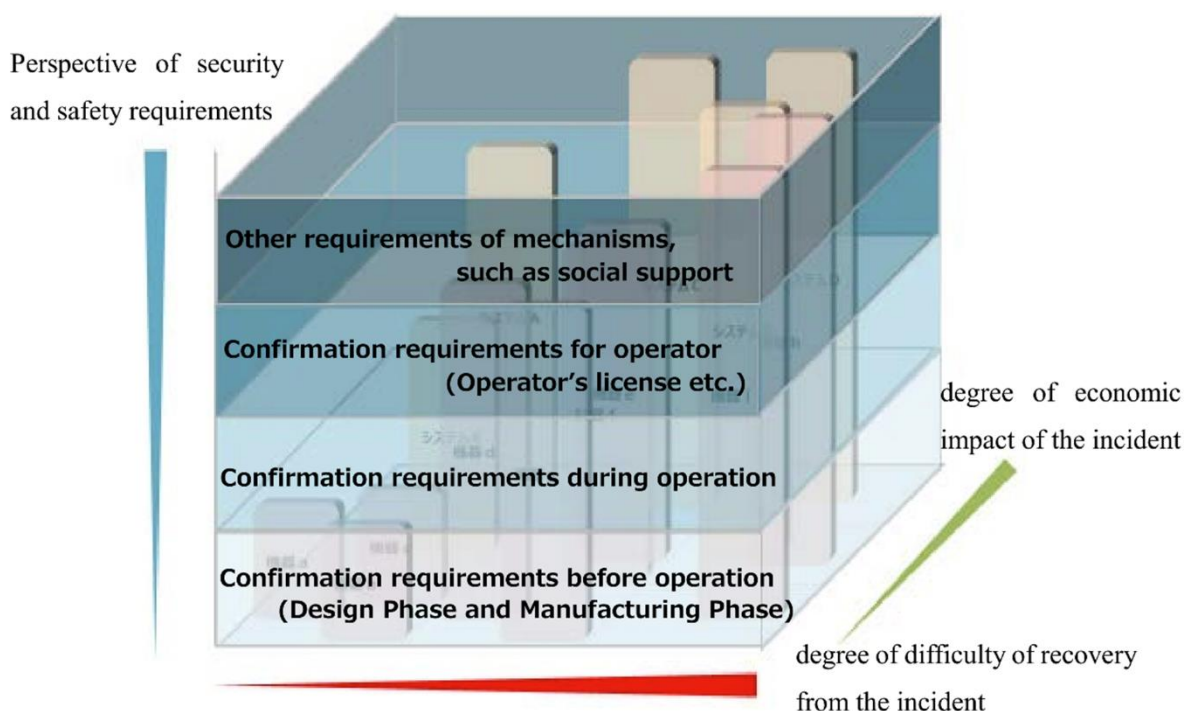
Source: Japan METI IoT Security Safety Framework

The framework then adds a third dimension covering the four security and safety requirements for dealing with these risks:

- Confirmation of requirements before operation (in design and manufacturing phases)
- Confirmation of requirements during operation (including clarifying the roles and responsibilities of stakeholders)
- Confirmation requirements for operators (including licensing service providers)
- Other requirements of mechanisms (including any “social safety net” such as mandatory insurance)

There is no assumption in the framework that there will be uniformity in the provision of security and safety for the multiple IoT devices and systems.

Figure 8: The perspective of security and safety requirements based on the category in Japan



Source: Japan METI

Japan's approach is interesting in its attempt to set up methods of analysis through classification of devices and systems. This approach assumes that these devices and systems will vary massively in use cases and recognizes that future use cases may yet be unknown.

The framework covers multiple standards and codes of practice from international bodies including NIST; ETSI; the UK's Department for Digital, Culture, Media and Sport (DCMS); the Internet Society (ISOC); and Japan's own regulations and working groups.

By its nature, it sets out voluntary rather than mandatory measures.

Also in 2020, the Ministry of Internal Affairs and Communications revised its Ordinance Concerning Terminals Etc., making internet access control functions mandatory, as well as functions that encourage the user to set appropriate usernames and passwords for access control as well as firmware update functions for IoT products connecting directly to the telecommunication carriers' networks. Terminal facilities must conform to technical standards under the Telecommunications Business Act, aiming to prevent wide-spread IoT malware infection.

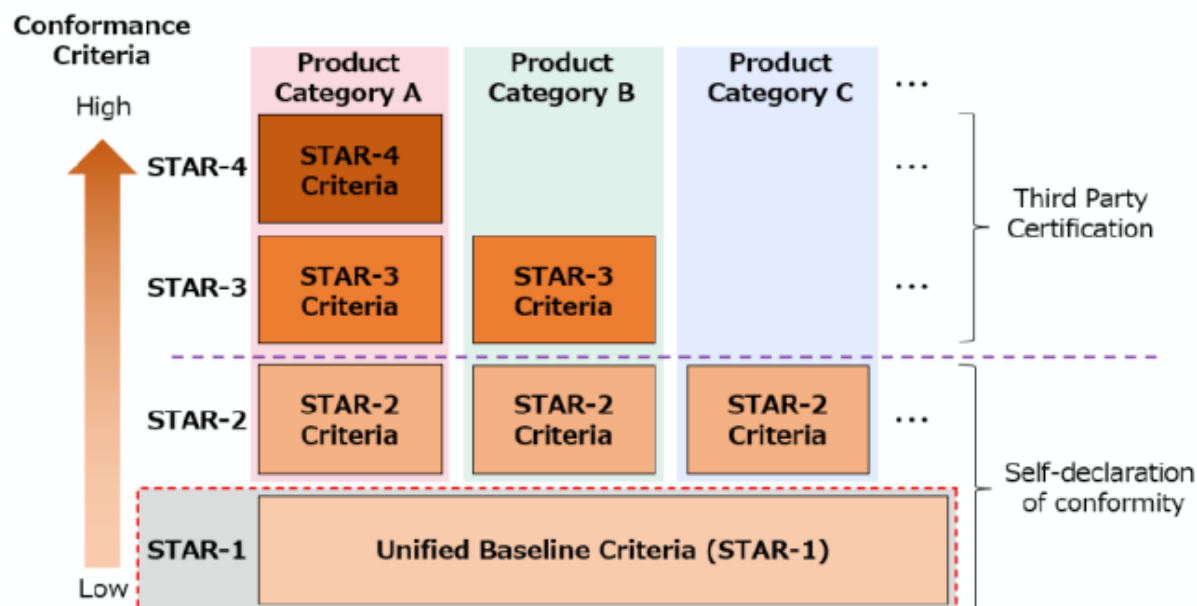
Similarly, the IoT Product Security Conformity Assessment Scheme will also be voluntary. The policy document for the scheme was published on August 30, 2024 by METI. The scheme aims to establish a framework to enhance the cybersecurity of IoT products through a labeling system, hoping that this label will become a procurement requirement for government agencies, critical infrastructure

providers, and local governments. For Japanese government agencies, the procurement of labeled products will be mandatory by the time they are widely used. It has been confirmed so far that security cameras, drones, firewalls, and routers will be expected for STAR-3 and above for procurement by government agencies. The Secretariat of the Scheme will work with relevant industry associations and working groups to establish sector-specific standards and labels, with priority given to critical infrastructure. It introduces four conformity assessment levels, known as STAR-1 to STAR-4 as follows:

- STAR-1: Baseline security, addressing threats common to all IoT products, assessed via a self-declaration of conformity by IoT product vendors.
- STAR-2 to STAR-4: Category-specific, which include stricter requirements tailored to specific product categories and critical sectors, with STAR-3 and above requiring third-party evaluation for certification by IPA-certified laboratories.

The labels for STAR-1 and 2 will be valid for up to two years, at which point a new declaration of conformity will be required, whereas for STAR-3 and above this will be considered after 2024.

Figure 9: Visual presentation of Conformity Assessment Levels



Source: Japan METI

While the scheme is not just focusing on consumer devices and expanding into critical infrastructure sectors, it draws inspiration from a number of standards and other government guidance/regulation. Overlapping requirements across standards and schemes were pulled out, including ETSI EN 303 645, NIST IR 8425, Singapore's CLS, UK's PSTI Act, and the European Cyber Resilience Act (profiled later in this report), with the aim of mutual recognition, as well as reference to ISO/IEC 27404. From all these overlapping requirements, Japan's requirements for each STAR level were pulled out.

The scope of the scheme includes devices that can be connected to the internet such as routers and security cameras, as well as those that can be connected to a network of other devices using IP such as hub and smart home devices as well as operational technology (OT) devices such as programmable logic controllers (PLCs), industrial control systems (ICS) sensors, and controllers. Smartphones are factored into "general-purpose IT products" and are not included.

The scheme is currently still in development, and METI have highlighted the need to consider overlap with both existing Japanese and international schemes, including Japan's Ordinance Concerning Terminal Facilities Etc. IPA, an administrative agency under METI, will establish the scheme in accordance with the policy as well as operate it. The security requirements and conformance criteria for STAR-1 have been determined, which aligns closely with ETSI EN 303 645, whereas the others are still in development. IPA plans to start accepting applications for STAR-1 as of March 2025, and the others later.

Singapore

In October 2020, the Cyber Security Agency of Singapore (CSA) launched its Cybersecurity Labelling Scheme (CLS) for consumer smart devices, claiming it as the first in the Asia & Oceania region.

Figure 10: Singapore's Cybersecurity Labelling Scheme label



Source: CSA

This scheme initially covered Wi-Fi routers and smart home hubs before being extended to include all categories of consumer IoT devices such as IP cameras, smart door locks, smart printers, and smart lighting. It is a voluntary scheme with four levels of labeling, indicating different levels of security rating:

- Tier 1 meets baseline security requirements (compliant with ETSI EN 303 645) documented through the developer's declaration of conformance.
- Tier 2 meets secure product lifecycle requirements (compliant with Singapore's IMDA IoT Cyber Security Guideline) documented through the developer's declaration of conformance.
- Tier 3 has had external software testing to find known vulnerabilities and software bugs. The tests must be done by a CLS-approved third-party laboratory.
- Tier 4 has undergone thorough security evaluation for ETSI EN 303 645 conformance as well as additional (and mandated) penetration testing. The tests must also be done by a CLS-approved third-party laboratory.

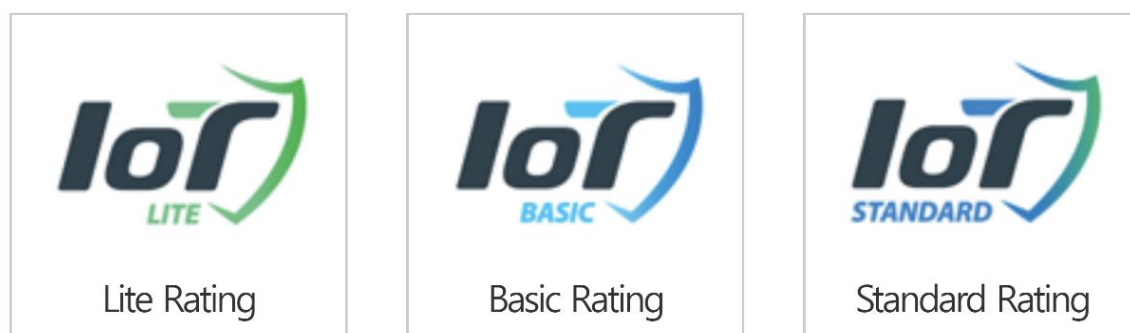
In October 2021, the CSA and the National Cyber Security Centre Finland signed a memorandum of understanding (MoU) for mutual recognition of each other's labeling schemes and associated processes. Since then, there have also been mutual recognition agreements established with Germany as well as South Korea.

In September 2023, the scheme had significant updates including a simplified application process and revised documentation requirements, updated requirements for binary scans under Tier 3 and 4, as well as assessment methodology publications to aid manufacturers and assessors.

South Korea

South Korea's Internet and Security Agency (KISA) has introduced a Certification of IoT Cybersecurity (CIC), which formally certifies IoT devices into three grades—IoT Lite, Basic, and Standard—with each having a different timeline for certification (anywhere from 6 weeks to more than 12 weeks) and different costs for each level of certification.

Figure 11: The three levels of South Korean IoT device security certification



Source: KISA

- Lite is the required level of security measures to respond to simple hacking attacks, which has 10 test items.
- Basic has a general level of security measures, aiming to block illegal access to data and prevent exposure. It has 29 test items.
- Standard looks for a comprehensive level of security to respond to advanced hacking attacks, including international requirements. It has 43–50 test items.

Authentication for the certificates is split across seven areas:

- Identification and authentication: The use of secure methods for managing permissions and authentication of users, as well as restricting unauthorized mutual authentication, limiting the number of attempts, preventing information disclosure, and securing sessions
- Data protection: Securing transmitted and stored data, extra protection for stored sensitive information, legal compliance with personal information, and the complete erasure of sensitive information

-
- Password: The use and management of cryptographic algorithms, the generation of secure encryption keys, and the generation of random secure numbers
 - Software security: Protecting and applying code, source code obfuscation, testing security features, addressing known vulnerabilities, avoiding unnecessary features and code, and providing audits of development
 - Update and technical support: Verifying product names and associated information, ensuring secure updates and recovery if updates fail, keeping technical support up to date, providing accurate update information, and automatic update of procedures
 - Operating system (OS) and network security: Providing a secure OS; limiting the number of unnecessary accounts, services, and ports; disabling unnecessary network interfaces; the verification of executable code and configuration files; system restoration on failure; response to denial-of-service attacks; the protection of OS functions; minimization of access rights; the blocking of unauthorized software installation, execution, and remote access; and network traffic control
 - Hardware security: Provision of the device's safe booting and self-testing, response to self-test and hardware failures, defense against tampering, responses to side-channel and memory attacks, and protection of nonvolatile memory and internal and external interfaces

Testing and certification are carried out by the Korea Institute of Mechanical, Electrical, and Electronic Testing (KTC) and the Korea Information and Communication Technology Association (TTA).

The CIC covers eight categories of devices, including home appliances, transportation, finance, smart city, medical care, manufacturing and production, housing, and telecommunications. The device, the cloud server or platform, and the IoT apps are in scope for certification.

South Korea's approach to IoT security is mainly aimed at manufacturers of components and ICT products. The scheme is voluntary, rather than required in South Korea.

Taiwan

The Taiwan Association of Information and Communications Standards (TAICS) issued its voluntary IoT Cybersecurity Mark, with the goal to enhance consumer confidence in the security of their devices, strengthen IoT cybersecurity as well as make international markets more accessible to Taiwanese manufacturers. Similar to other countries, the idea is that the security products will be preferentially procured by public organizations in Taiwan. The test specifications first focused on wired/wireless network cameras, owing to their relation to personal privacy, with corresponding cybersecurity standards and test specifications for other IoT devices developed afterward. Its Video Surveillance System Cybersecurity Standard is certified as a national standard (CNS 16120), jointly developed by TAICS and the Institute for Information Industry (III).

That said the scheme does aim to have international interoperability. TAICS uses accredited laboratories for certification, some of which are international service providers. TAICS has also suggested testing and certification to international standards such as ETSI and MTSFB (Malaysian Technical Standards Forum Bhd).

Its “Security assessment guidelines for IoT-enabled field applications” covers four major assessment processes: threat modeling; vulnerability testing; penetration testing; and impact analysis across the sensor layer, network layer and application layer.

Both products with wired interfaces and telecommunication/communication devices with wireless interfaces are in scope. The mark has various security levels based on the level of risk and the complexity of cybersecurity protection technology divided into three security levels:

- Level 1, suitable for general household use
- Level 2, suitable for commercial use
- Level 3, maximum protection

The above correlates to stars, and graphics, from Basic 1 star, Intermediate 2 stars, and Advanced 3 stars, shown in **Figure 12** below.

Figure 12: Taiwan IoT Cybersecurity Mark

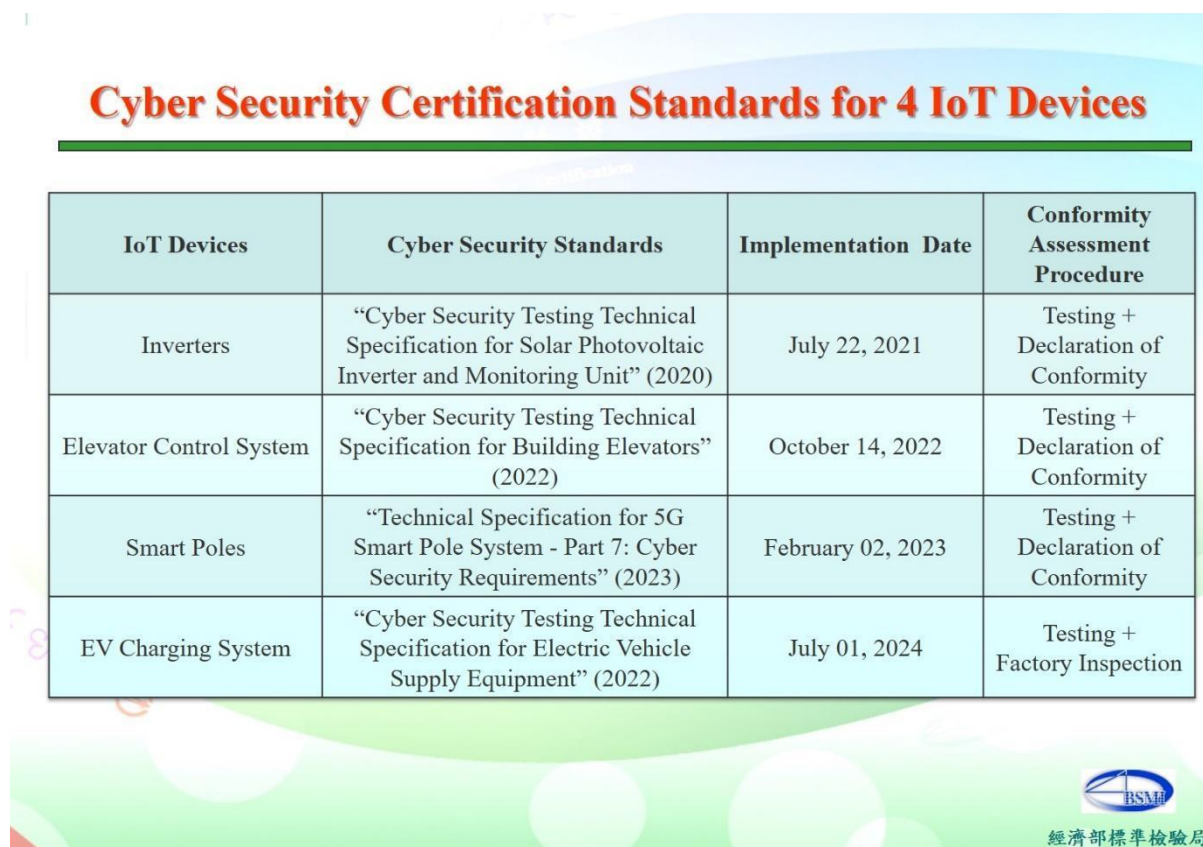
	Basic 1 star	Intermediate 2 stars	Advanced 3 stars
Graphic			
Security level	Level 1	Level 2	Level 3
Description	Suitable for general household use	Suitable for commercial use	Maximum protection

Source: TAICS

Although not all focused on consumer IoT devices, the Bureau of Standards, Metrology and Inspection (BSMI) has added cybersecurity requirements within certification for four types of IoT devices to its Voluntary Product Certification program: smart poles, renewable energy system inverters, electric vehicle (EV) charging systems, and elevator control system equipment. These certification standards are harmonized with international standards, spanning:

- Physical security
- System security
- Firmware updates
- Communication security
- Identity

Figure 13: How these standards were implemented



IoT Devices	Cyber Security Standards	Implementation Date	Conformity Assessment Procedure
Inverters	“Cyber Security Testing Technical Specification for Solar Photovoltaic Inverter and Monitoring Unit” (2020)	July 22, 2021	Testing + Declaration of Conformity
Elevator Control System	“Cyber Security Testing Technical Specification for Building Elevators” (2022)	October 14, 2022	Testing + Declaration of Conformity
Smart Poles	“Technical Specification for 5G Smart Pole System - Part 7: Cyber Security Requirements” (2023)	February 02, 2023	Testing + Declaration of Conformity
EV Charging System	“Cyber Security Testing Technical Specification for Electric Vehicle Supply Equipment” (2022)	July 01, 2024	Testing + Factory Inspection

BSMI
經濟部標準檢驗局

Source: Taiwan BSMI

Thailand

In Thailand, the Office of the National Broadcasting and Telecommunications Commission (NBTC) is in the process of establishing security regulations for IoT devices. Its National Cyber Security Agency (NCSA) has established a Cybersecurity Act, including 40 new subordinate regulations mainly to cover the hundred or so organizations that form part of Thailand's critical information infrastructure.

The Personal Data Protection Act (PDPA) implemented in 2022 is like the EU's GDPR, covering data collection, processing, storage, consent, and protocols as well as cross-border data transfer and data deletion and anonymization most recently. It also applies to all organizations that collect, use, or disclose personal data in Thailand or about Thai residents, regardless of their location across the globe.

Vietnam

IoT is important in Vietnam; in 2019, it set up an IoT information hub with Ericsson in Hoa Lac Hi-Tech Park in Hanoi.

In May 2021, the government's Authority of Information Security (AIS) announced its "Decision No. 736/QĐ-BTTTT setting out the List of Baseline Requirements to Ensure Cyber Security for Consumer IoT Device." It is a voluntary scheme for manufacturers, with specifications similar to ETSI 303 645, and sets out baseline security requirements for IoT devices.

The country's constitution (Constitution 2013 and Civil Code 2015) contains fundamental principles of rights to "privacy, dignity, and honor." The collection, use, storage, processing, and disclosure of personal information are covered in several laws and guidelines.

Europe

The European Union (EU)

The EU is by far the largest government organization in Europe, with a GDP of \$14.5tn and a population of 450 million in 2021. Like much of its legislation, IoT device security is established at a central level before being implemented by each member state. There are a number of EU specifications related to IoT security. Some examples are given below.

The Radio Equipment Directive

In October 2021, the EU supplemented its Radio Equipment Directive (RED) 2014/53/EU to ensure network protection, safeguards for the protection of personal data and privacy, and protection against fraud, specifically to recognize the growing importance and use of IoT devices. The new requirements were originally planned to be mandatory from August 2024, but this was extended to August 2025. In general, the act focuses on:

- Improving network resilience by requiring features that prevent communication being harmed or disrupted, website disruption, and loss of service functionality
- Protecting consumers' privacy, including the protection of children's rights and prevention of unauthorized transmission of or access to personal data

-
- Reducing the risk of monetary fraud, focusing on better authentication and control when monetary payments are made

In November 2022, the EU published Commission Implementing Decision 2022/2191 aimed at harmonizing standards for radio equipment and drafted in support of Directive 2014/53/EU. The decision is now in effect and implements harmonized standards in support of the Radio Equipment Directive.

A series of three standards have been developed by CEN/CENELEC under the mandate of the European Commission to support the RED cybersecurity essential requirements, EN 18031 series, but they have not yet been harmonized. These have been developed by CEN-CENELEC Joint Technical Committee 13 and need to be purchased, arguably limiting their accessibility.

- EN 18031-1 – Part 1: Internet-connected radio equipment
- EN 18031-2 – Part 2: Radio equipment processing data, namely internet-connected radio equipment, childcare radio equipment, toy radio equipment, and wearable radio equipment
- EN 18031-3 – Part 3: Internet-connected radio equipment processing virtual money or monetary value

On January 30, 2025, the standards were harmonized, with the references published in the Official Journal of the EU, meaning the standards can be presumed to be in conformity with the essential requirements set out in Article 3 of the directive. That said, there are several caveats and areas which are lacking, resulting in the references being published with restrictions.

- The three above standards include sections named “rationale” and “guidance” do not set out specifications, and the guidance section refers to other standards that should not be included in harmonized standards as a general rule.
- The password section of the standards would give manufacturers the possibility to allow a user to not have or set a password. This does not conform with the essential requirements set out in the directive and would not properly deal with authentication risks.
- The relevant authentication risks also might not be addressed with the specifications on access control for toy radio equipment and childcare radio equipment in EN 18031-2.
- Assessment criteria for secure updates in EN 18031-3 do not properly address the relevant authentication risks and, thus, do not ensure conformity with the requirements in the directive. There are a few methods listed for implementing secure updates, but none of these alone would be sufficient for financial assets.

The GDPR Directive

Personal data created, stored transmitted, and processed by IoT devices is subject to GDPR Directive 95/46/EC (May 2018). This includes the right to be forgotten, the requirement for clear requests for

content for data collection and processing, and heavy financial penalties for noncompliance. GDPR applies to data pertaining to EU citizens, irrespective of where that data is held—meaning requirements will apply to organizations even outside of the EU. GDPR has become a worldwide catalyst for data privacy and has inspired many other countries and states, including the California CPRA (Privacy Rights Act) in 2020.

The Network and Information Security Directive

The IT infrastructure that devices are connected to is covered by Network and Information Security (NIS) Directive (May 2018). This specifies high-level cybersecurity requirements for critical national infrastructure and essential services, including digital services providers.

The directive requires member states to set up competent authorities with which service suppliers can interact. A new legislative proposal, NIS2, was agreed on in May 2022. NIS 2 came into force in the EU on January 16, 2023. It builds on and has replaced the existing directive. NIS 2 will modernize the legal framework to consider the increased digitization of the internal market and the evolving cybersecurity threat landscape. It applies to a broader scope of sectors and companies and focuses mainly on the four areas of risk management, corporate accountability, business continuity, and reporting. Minimum cybersecurity measures include a number of measures from supply chain security to incident response planning and access control.

The deadline for member states to transpose NIS 2 into their national legislative framework was October 17, 2024. That said, many member states have faced delays in transposing this into national law. ENISA has worked on several supporting documents, including developing technical guidance to support EU member states and entities with the implementation of the risk-managed measures outlined in the regulation as of October 17, 2024, as well as an assessment of the impact of current EU cybersecurity framework, particularly the NIS 2 Directive.

The Cybersecurity Act

The business services accompanying IoT devices, and the devices themselves, are covered by the EU's Cybersecurity Act (2019/881, 2019). This grants a mandate to ENISA to help member states address cybersecurity threats, increase operational cooperation at an EU level, and coordinate the EU in case of cross-border attacks and crises. ENISA is in the process of building an EU-wide European cybersecurity framework for ICT products, services, and processes, which will be validated by the EU before being recognized at the country level. ENISA's certification schemes will initially be voluntary.

Medical Device Regulation

Medical IoT devices are covered by the EU's Medical Device Regulation (MDR 2017/745), which applies stricter standards for medical devices throughout their lifecycles, including conformity assessments. This entered into force in May 2021. In addition, the IVDR 2017/746 covers in vitro diagnostic medical devices, which entered into force in May 2022.

The above specifications are applicable in most cases to the European Economic Area (EEA), which includes Iceland, Liechtenstein, and Norway in addition to the 27 EU countries. The UK is currently following the EU's approach, although its withdrawal from the EU and the EEA at the beginning of

2020 will potentially lead to future divergence. The legislation applies to both domestic and foreign (e.g., US and Asian) manufacturers alongside local and international service providers.

The European Commission is aware that despite considerable progress in transitioning to the new rules, it remains slow. It is taking additional steps to ensure the availability of high-risk in vitro devices by May 2025, thereby extending the transition period to December 2027 for high-risk and 2028 and 2029 for medium- and lower-risk devices.

The Cyber Resilience Act

The Cyber Resilience Act addresses market needs and “protects consumers from insecure products by introducing common cybersecurity rules for manufacturers and vendors of tangible and intangible digital products and ancillary services.” It covers products with digital elements used by both enterprises and consumers, including consumer IoT. The act ensures that:

- Wired and wireless products connected to the internet, as well as software, are more secure and have fewer vulnerabilities
- Manufacturers will need to be responsible for the cybersecurity of the product, specifically throughout its whole lifecycle
- Consumers, and enterprises, can make informed purchasing decisions based on cybersecurity of the products.

Businesses and consumers will thus have better protection.

Devices with digital elements are divided into criticality categories: “Class I and Class II Important” products, “Critical” products, and then everything else with digital elements. Some categories will be subject to self-assessment rather than third-party involvement. The definition of these categories has changed over time with the development of the final text of the regulation. For the most part, consumer IoT devices are not listed in the important or critical categories, except for smart home assistants; smart home devices with security functions such as door locks, cameras, baby monitoring, and alarms; and internet-connected toys that have interactive or location tracking features.

In addition to the areas above, manufacturers’ obligations include:

- Ensuring cybersecurity through planning, design, development, production, delivery, and maintenance
- Having documentation on all risks and reporting all actively exploited vulnerabilities and incidents for the expected product lifetime or for five years, whichever is shorter
- Providing clear and understandable instructions for use, with a support period for security updates of at least five years

The act was approved by the European Parliament on March 12, 2024, and adopted by the Council on October 10, 2024. It will become fully applicable by December 11, 2027, with some reporting requirements required earlier from September 11, 2026.

EU standards based on the CRA will be created to help with implementation, including the essential requirements set out in the regulatory text. The text states that existing European and international standards will be considered for simplification purposes.

Finland

Finland introduced a cybersecurity label in 2019 to showcase whether the features of a product or service has been implemented in a secure manner. The device was in scope as well as the device's ecosystem—extending to applications and cloud. The scheme is managed by the Finnish Transport and Communications Agency (Traficom) and has mutual recognition with Singapore's scheme.

Requirements broadly align with ETSI EN 303 645, covering the following areas:

- Passwords
- Software updates
- Data protection
- Secure transfer and storage of data
- Secure default settings

Those seeking to obtain a Cybersecurity Label have to fill in a statement of compliance, then the National Cybersecurity Centre Finland (NCSC-FI) reviews the information, following which an independent third party inspects the product or service, compared against the requirements. The label is eventually granted by the NCSC-FI.

As of 2025, Traficom has announced that it has stopped issuing new Cybersecurity Labels, given the EU-wide regulations for connected devices—the RED and CRA. Traficom has made this decision as it believes the significance of its label will lessen with the new regulations entering into force.

France

In France, cybersecurity is part of the remit of the National Information System Security Agency (ANSSI), which reports to the Secretariat-General for National Defense and Security (SGDSN), itself reporting to the prime minister. It was the leader in drawing up the country's digital security strategy in 2015, which is based on five principles:

- Provide the defense and security of the state's information systems and critical infrastructure against major cyberattacks
- Provide digital trust and protection of privacy and personal data against cybercriminals

-
- Raise awareness and provide initial training and ongoing education in the subjects
 - Address cybersecurity within the context of technology businesses, industrial policy, export trade, and international markets
 - As a member of the EU, work to promote a safe, stable, and open cyberspace

In 2018, ANSSI implemented a certification scheme. The scheme grants cybersecurity providers “security visas” to signify compliance with certification requirements. The scheme covers three areas:

- Regulatory – meeting French and EU legislation that enforce the use of cybersecurity solutions that guarantee tried and trusted levels of robustness
- Contractual – providing public and private organizations with documentation for the solutions they acquire
- Commercial – providing product and service providers and users of their offerings with the competitive advantages of meeting the scheme’s cybersecurity criteria

There are two levels of certification:

- Certification de Sécurité de Premier Niveau (CSPN) – a process that takes around two months and 25–35 person-days; the less exhaustive of the two levels, it places more emphasis on product analysis to estimate its resistance to a moderate level of attack
- Common Criteria (CC) – an international (ISO/IEC 15408) of a product’s security based on assessments of the product within its development environment and resistance to a given potential attack with seven assurance levels

Consumer IoT devices are not specifically called out in the reference material, although they are part of the agency’s “Recommendations on the Security of Connected (systems) Objects” published in August 2021.

Germany

Germany is very sensitive about the protection of personal information and privacy. In December 2020, the government passed a draft of the Second Act to Increase the Security of Information Systems (IT Security Act 2.0). It is designed to protect the federal government and critical infrastructure organizations from cybercrime. The threshold for defining critical infrastructure has been lowered, increasing the number of organizations classified and requiring them to implement stricter measures as well as mandatory reporting. It also includes new obligations for supply chain security.

Figure 14: An example of a German BSI IT security label



Source: BSI

Germany's Federal Office for Information Security (BSI, not to be confused with the UK's British Standards Institute) introduced a voluntary IT security-labeling scheme in January 2022. It allows the manufacturer to declare compliance with:

- German technical guidelines (such as BSI TR-03148 for secure broadband routers)
- ETSI standards (such as its Cyber Security for Consumer Internet of Things: Baseline Requirements – ETSI EN 303 645)

These are based on a test specification adhering to the associated standards.

BSI publishes a website that provides detailed information on the security of the product. The website link is provided as part of the security label on the IoT device. Information on the site includes how patches will be applied to close security flaws and how cryptography is used to protect communications and data storage.

Suppliers need to file an application and submit a declaration of compliance with the BSI product category's requirements. Once this is granted, the supplier will receive a time-limited label assigned to the product and its associated product information web page. Although this self-certifying labeling scheme is voluntary for suppliers, compliance with appropriate cybersecurity and privacy guidelines is not.

The German approach is currently based on this voluntary self-certifying labeling scheme for IoT manufacturers and service providers, but more sophisticated and compulsory schemes will be

introduced in future as the threats across the continent increase and the European guidelines and standards mature.

There is a mutual recognition agreement between Germany's BSI and Singapore's CSA, discussed above, with Germany's label recognized as meeting Singapore's Cybersecurity Labelling Scheme Level 2 standards, and vice versa.

In addition, BSI also has the Beschleunigte Sicherheitszertifizierung (BSZ), a fixed-time cybersecurity certification for IT products. The BSZ implements the European Standard EN 17640 (published by CEN/CENELEC) fixed-time cybersecurity evaluation methodology for ICT products. While the initiative does not cover all IoT devices, it does include general network components and embedded IP-networked devices in scope. There is a mutual recognition agreement between BSZ and the French CSPN certificates, with a new logo being used as of August 2024, as well as the Spanish Lightweight Information and Communication Technology Product security evaluation (LINCE) and Dutch Baseline Security Product Assessment (BSPA).

Spain

The Spanish government implemented its National Cybersecurity Strategy in 2019, replacing its first 2013 version. It includes several of ENISA's goals, including how to deal with cybercrime, protecting critical national infrastructure, incident response, cybersecurity exercises, and education and training programs. At the beginning of 2021, it also published its Plan Nacional de Competencias Digitales, which is designed to increase the digital (including cybersecurity) skills of subject matter experts and government.

Spain's national security legislations include:

- Law 34/2002 on services to the information society and e-commerce
- Law 25/2007 on data retention in electronic communications and public communications networks
- Organic Law 15/1999 on data protection
- Basic Law 3/2018 – Spanish data protection law implementing the EU's GDPR legislation
- Royal Decree Law 12/2018 and 43/2021 (regarding the notification of security breaches) implementing the NIS Directive

Spain has two cybersecurity response organizations:

- The National Cybersecurity Institute (INCIBE), set up in 2008, reports to the National Center for the Protection of Critical Infrastructure (CNPIC). It has national responsibility for the general public, businesses, and other organizations. It published its "Security of Installation of Internet of Things (IoT) Devices" guide in 2020, covering how criminals can take advantage of devices, and the measures that organizations can take to minimize the risks of suffering associated security incidents.

-
- The National Cryptologic Center (CCN), which is part of Spain's National Intelligence Center, covers government institutions. It is responsible for strengthening national cybersecurity by responding to cyberattacks and raising awareness of relevant issues.

Spain's current approach is to raise awareness of the issues rather than legislate on how IoT products and associated services are implemented. It does not yet have compulsory certification or schemes for consumer IoT device security. However, CCN has developed LINCE, a methodology for evaluating and certifying ICT security products. There is a basic evaluation as well as other modules for higher assurance levels. The certification aims to be more accessible, completed in a short amount of time, yet focusing on testing security functionality against the most relevant vulnerabilities and threats. While this is not mandatory for all products, it is a requirement for products used by Spain's administration and CNN. The certification is not intended for highly critical products, only those with low or medium criticality.

The UK

In November 2021, the UK's Department for Digital, Culture, Media and Sport (DCMS) introduced the Product Security and Telecommunications Infrastructure (PSTI) Bill, which became the PSTI Act on December 6, 2022. The measures of the first part include:

- Ensuring that consumer connectable products, such as smart TVs, internet-connectable cameras, and speakers, are more secure against cyberattacks, protecting individual privacy and security
- Requiring manufacturers, importers, and distributors to comply with new security requirements relating to consumer connectable products
- Creating an enforcement regime with civil and criminal sanctions aimed at preventing insecure products from being made available on the UK market

The terms of the PSTI were drawn up through a formal consultation project with the National Cyber Security Centre, industry, consumer groups, and academia, and are designed to help to apply security to an area that is growing rapidly and is currently insecure.

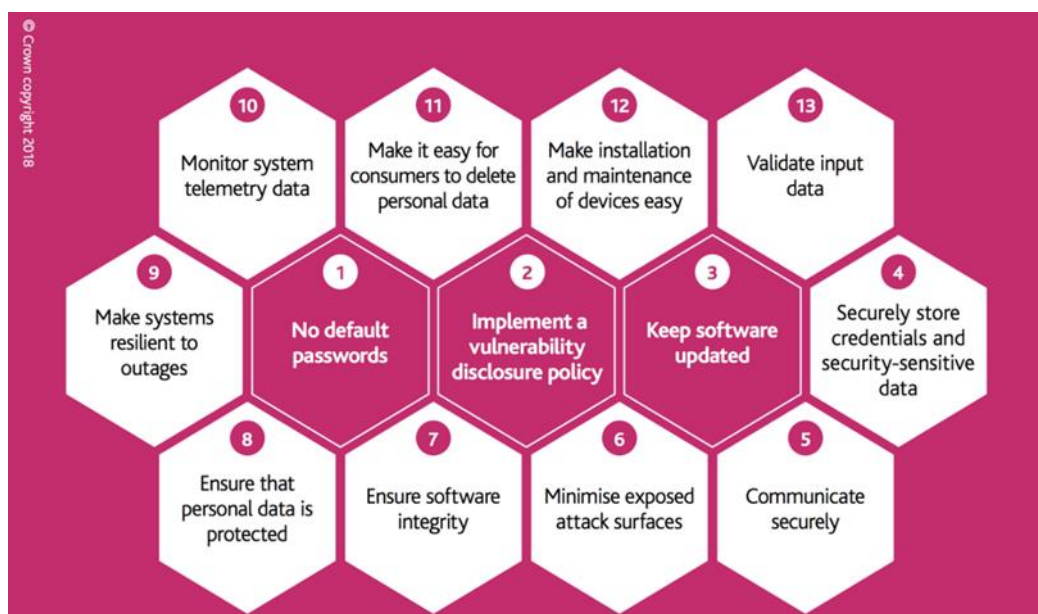
The second part of the act is designed to speed up the rollout of gigabit-capable broadband and 5G networks across the country.

The product security requirements became mandatory as of April 29, 2024 for business in the supply chain. Of the 13 requirements indicated by the UK Code of Practice for Consumer IoT Security (below), the specific requirements that must be complied with are:

- No default passwords, which must be unique per product and capable of being defined by the user
- The manufacturer must provide clear, accessible, and transparent information on reporting security issues as well as the timelines for acknowledgment and status updates through to resolution.

- The consumer must be able to access information on minimum security update periods with an end date of support.

Figure 15: The UK's DCMS Code of Practice for Consumer IoT Security covers 13 areas



Source: DCMS

The UK has based its approach on its publication in 2018 of a code of practice (above) that is largely consistent with ETSI's 303 645 13 requirements. It has not yet introduced a compulsory certification process or labeling scheme. However, it does mention that a Statement of Compliance must "accompany" the product and defines this as a document.

Americas

Brazil

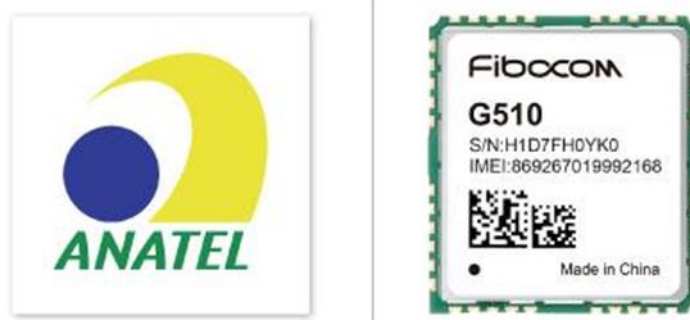
Brazil has recognized the importance of IoT, signing its National Plan of IoT into law in 2021. It also recognized the importance of data privacy in a similar way to the EU's GDPR. The General Law of Personal Data Protection (LGPD) became law in 2020, along with sanctions that would be applied by the National Data Protection Authority (ANPD) for violations.

Brazil's LGPD states that companies can only collect personal data with the consent of users, who can request access to their data and demand its complete erasure at any time. Penalties for violations of LGPD range from warnings, substantial fines (including fines based on revenue or daily penalties), to partial or full suspension of operations.

To enforce the execution of Brazil’s national plan, a Chamber for Management and Monitoring of Machine-to-Machine and Internet of Things Communication Systems Development (Câmara IoT) was also created.

In July 2021, Brazil’s Cyber Security Requirements for Telecommunications Equipment Act (Act 77) came into force, mandating that products “with a terminal equipment function with internet connection or telecommunications network infrastructure equipment must submit a statement of the interested party stating which requirements listed in the document the product and its supplier meet.” As with many other countries, ETSI EN 303 645 is also referenced.

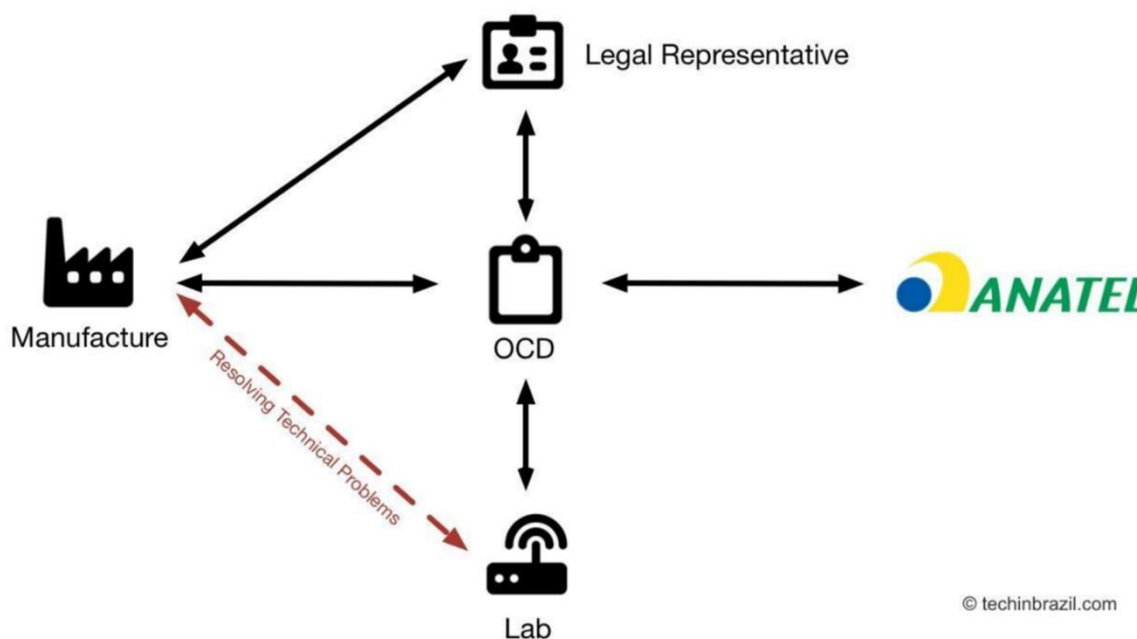
Figure 16: An example of a Brazilian Anatel Certificate of Conformity label



Source: Anatel

Certificates of Conformity for ICT products are issued by a designated certification body (an OCD), indicating that they comply with and have been authorized by the Brazilian Telecommunications Agency (Anatel). OCDs check the technical characteristics of the product, determine the applicable regulations, and perform the laboratory tests specified for the certification and approval process. For imported products, the manufacturer must have a local representative responsible for product supply and warranty in Brazil. Sanctions for noncompliance are applied by the ANPD.

Figure 17: Anatel Certificate of Conformity homologation workflow for manufacturers without a legal entity in Brazil



Source: Anatel

Brazil also follows a Ministry of Science, Technology, Innovations and Communications (MCTIC) decree, Decree 9854/19, published as the Brazilian National Plan for IoT in 2019, which covers four areas for action: human capital, innovation, regulation, and technology. The aims are to keep the risks of technologies low and to protect privacy.

The US

As noted earlier, NIST has been a key player in establishing US cyber requirements. The organization is chartered to “advance measurement science, standards, and technology in ways that enhance economic security and improve [US] quality of life.” The agency has published several documents including a 2022 paper, “Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products,” and has thus been involved in the creation of the US’s cybersecurity labeling program, the U.S. Cyber Trust Mark.

NIST has been active in addressing the need for consumer IoT security. Then-president Joe Biden’s executive order (EO) on “Improving the Nation’s Cybersecurity (14028)” issued May 2021 called on NIST to:

- Publish guidance referencing “standards, procedures, and criteria”
- Initiate two security-labeling programs related to IoT and software

Since then, NIST has published essays, profiles (e.g., NIST IR 8425), and other documents and runs IoT cybersecurity workshops.

It has also published its NIST IR 8259 “Foundational Cybersecurity Activities for IoT Device Manufacturers,” which sets out six techniques manufacturers can use to add security capabilities to IoT devices.

Inspired by Energy Star, a labeling program operated by the Environmental Protection Agency and the Department of Energy to promote energy efficiency, the White House has adopted a voluntary IoT labeling program. This originally had a 2023 launch target, although it was eventually adopted in March 2024. The Federal Communications Commission (FCC) released the Cybersecurity Labeling for Internet of Things Report and Order, establishing the framework for the program with the rule effective as of August 29, 2024.

A number of Cybersecurity Label Administrators (CLAs) have since been announced in December 2024, responsible for the use of the label and the U.S. Cyber Trust Mark as well as day-to-day management of the program. UL Solutions has been conditionally approved as a CLA and as the Lead Administrator. UL Solutions, as Lead Administrator, will lead the 90-day stakeholder process (as of December 4, 2024) and develop a consumer outreach campaign with stakeholders to reach a set of recommendations. These need to cover the following three areas and a committee will be created to address each:

- The technical standards and testing procedures for at least one class of IoT products
- How a given class of IoT products must renew their requests to use the label
- The design of the label

As of March 4, 2025, the Lead Administrator, UL, was given a 60-day extension (until May 3, 2025) to ensure its recommendations are thoroughly considered and discussed among stakeholders.

The Cyber Trust Mark was launched on January 7, 2025.

The initiative, described as “Energy Star for cyber,” is intended to help Americans quickly and easily recognize whether devices meet a set of basic cybersecurity standards devised by NIST and the Federal Trade Commission (FTC).

The labeling program comprises two parts: the U.S. Cyber Trust Mark and a QR code, which directs consumers to a registry with specific information about the product, assuring the consumer that minimum cybersecurity standards have been met.

Figure 18: The U.S. Cyber Trust Mark label



Source: FCC

The order initially establishes the IoT Labeling Program will be for wireless consumer IoT products that can be internet-connected. Aligning closely with the NIST, the focus is specifically on “products” rather than just the device itself, extending to full functionality whether that be one or more IoT devices or additional components such as backend, gateway, or mobile apps necessary to use the device. Testing labs will test and assess IoT products for a fee, recognizing those accredited to ISO/IEC 17025 standards by the CLAs to conduct compliance testing that would support obtaining the label.

The NIST Core Baseline serves as the basis of the label’s requirements, including the following IoT product capabilities, as well as broad support for the technical criteria in NIST IR 8425:

- Asset identification
- Product configuration
- Data protection
- Interface access control
- Software update
- Cybersecurity state awareness

And the following IoT developer activities:

- Documentation
- Information and query reception

-
- Information dissemination
 - Product education and awareness

The Lead Administrator will develop and identify IoT cybersecurity standards and testing procedures that will meet the NIST IR 8425 criteria. This is likely to be a package of standards for each product type or class.

Additionally, in the last cybersecurity-related EO from the Biden administration, “Strengthening and Promoting Innovation in the Nation’s Cybersecurity” (14144), it states that the Federal Acquisition Regulatory (FAR) Council shall take steps to adopt requirements for agencies to require the Cyber Trust Mark on consumer IoT products sold to the federal government by January 4, 2027.

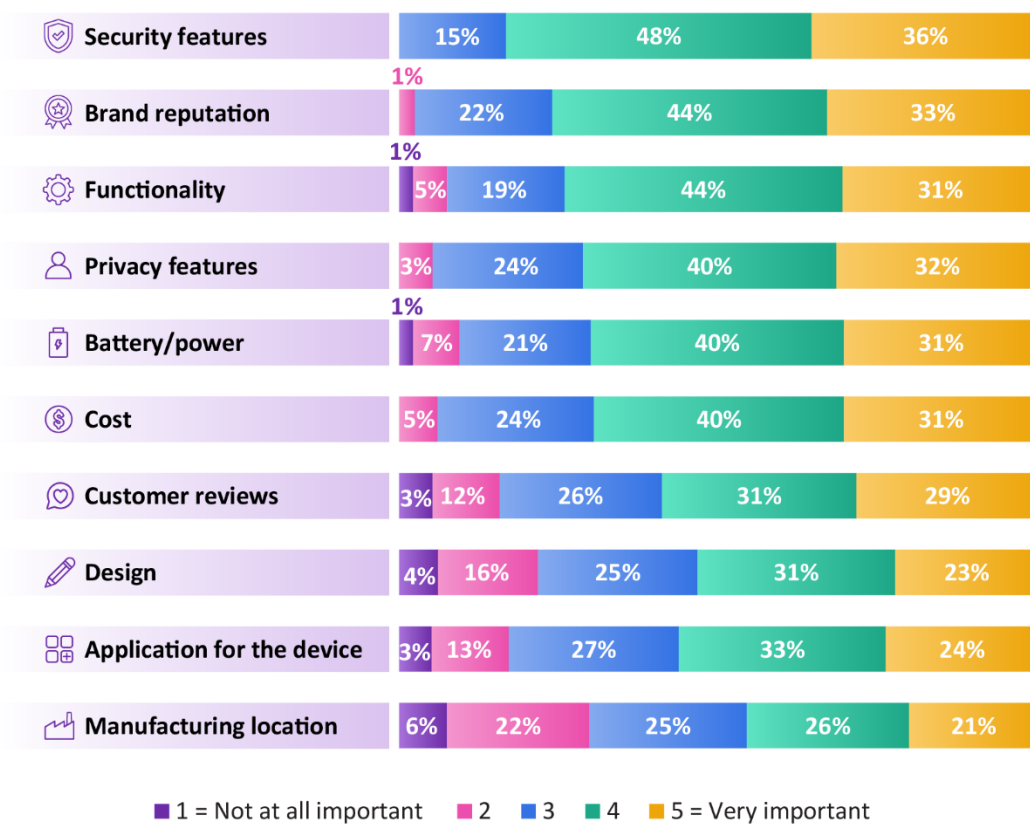
Part 2: Voice of the consumer

To support the initial publication of this report, Omdia conducted a survey of more than 400 consumers across 14 countries to assess their awareness and concerns regarding connected-device security. The study also assessed their awareness of standards and regulations and their interest in labeling schemes.

Security features were the most important purchasing attribute according to the survey: 84% of those surveyed cited this as important or very important. No respondents considered security unimportant. The next attribute, brand and reputation of the manufacturer, was considered important or very important by 77% of respondents. This overwhelming focus by consumers on security is critical. Manufacturers, standards organizations, and governments should take note and consider this a compelling case to act to address consumer expectations in this area.

Figure 19: Security is the most important purchasing attribute

Most important attributes when purchasing a connected device



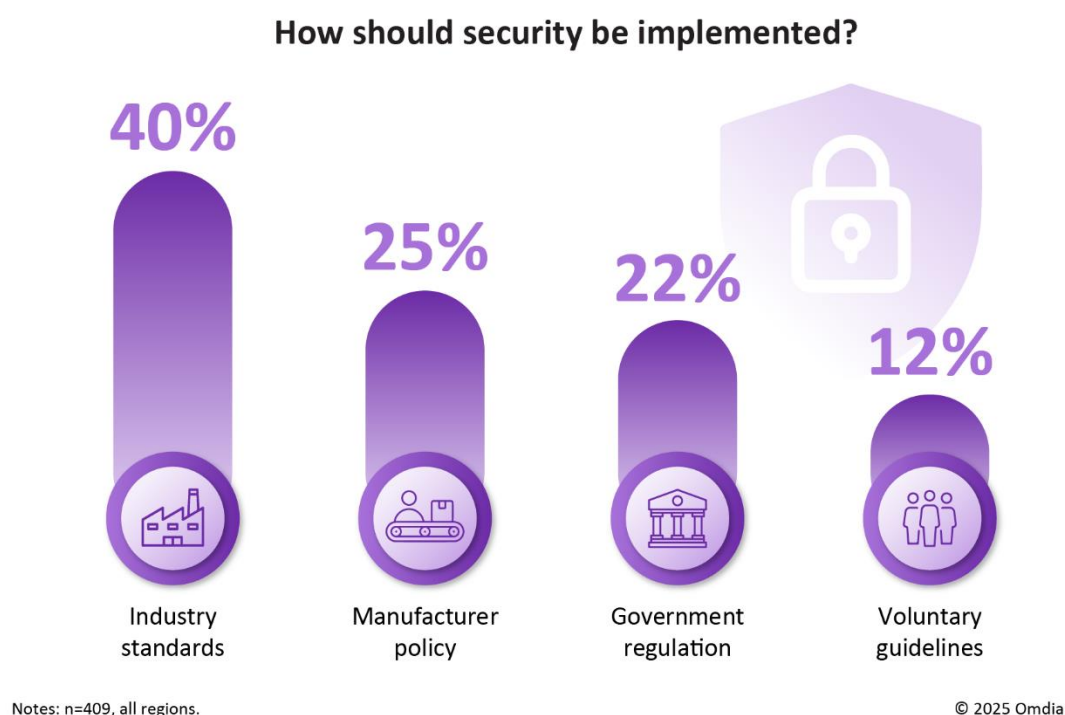
Notes: n=409, all regions.

© 2025 Omdia

Source: Omdia

When respondents were asked where and how security should be implemented, industry standards ranked highest. Manufacturers were cited second and, therefore, must step up to their responsibilities in this area.

Figure 20: How security should be implemented



Source: Omdia

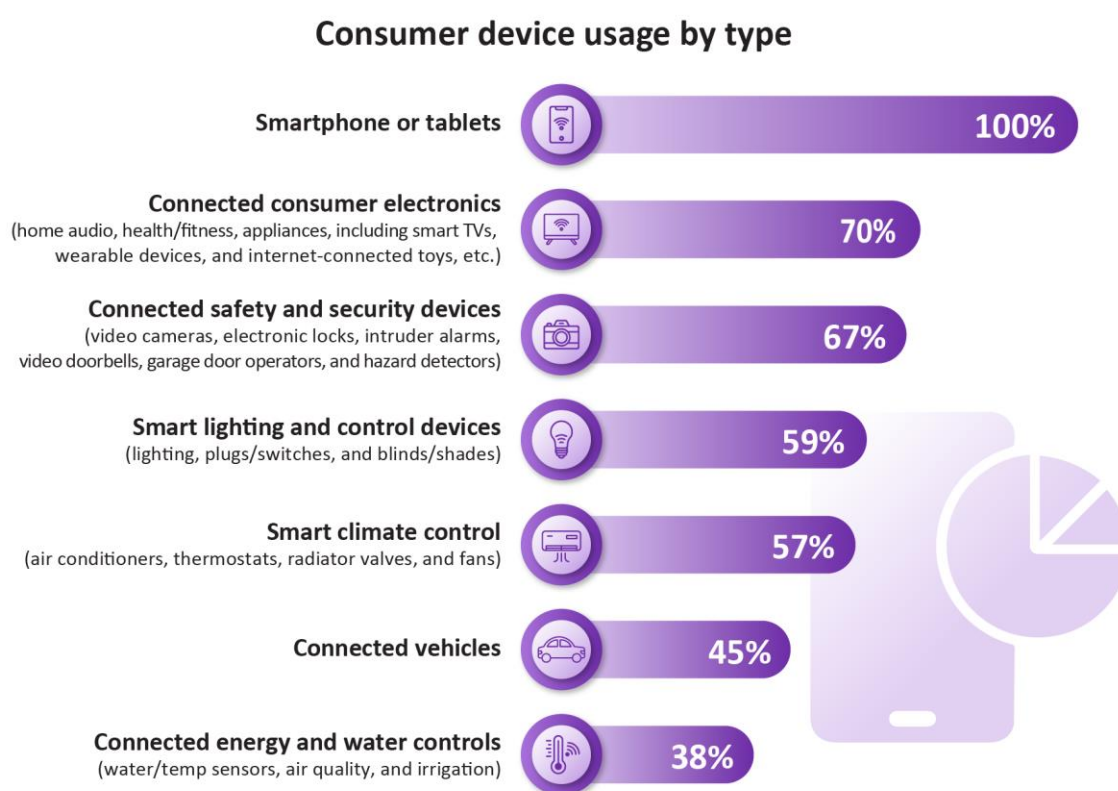
Equally interesting is that government regulations were cited next, only 3 percentage points lower than manufacturers, suggesting that even with standards and manufacturer compliance, the government, regulators, and policymakers should be considered the key stakeholders in the process.

Interestingly, there were some differences in responses by country. For example, consumers in Germany placed government regulation first, whereas consumers in the US more strongly supported manufacturer policy.

The majority of consumers surveyed reported using a variety of connected devices, with most using between 1 and 10 devices (89%) and only 11% using between 11 and 20 devices. Although all users reported using mobile phones and tablets, electronics and safety devices were also in high utilization, and more than half of respondents reported using “smart” and connected devices that provide comfort and convenience, such as lighting, blinds, and temperature control products. This highlights the need for an IoT cybersecurity posture to consider the wide array of device types in use. A one-size-fits-all approach or bias toward either end of the product complexity spectrum will

not be suitable to mitigate security risks effectively and efficiently across the array of products now in use.

Figure 21: Most respondents use comfort, convenience, and safety smart products



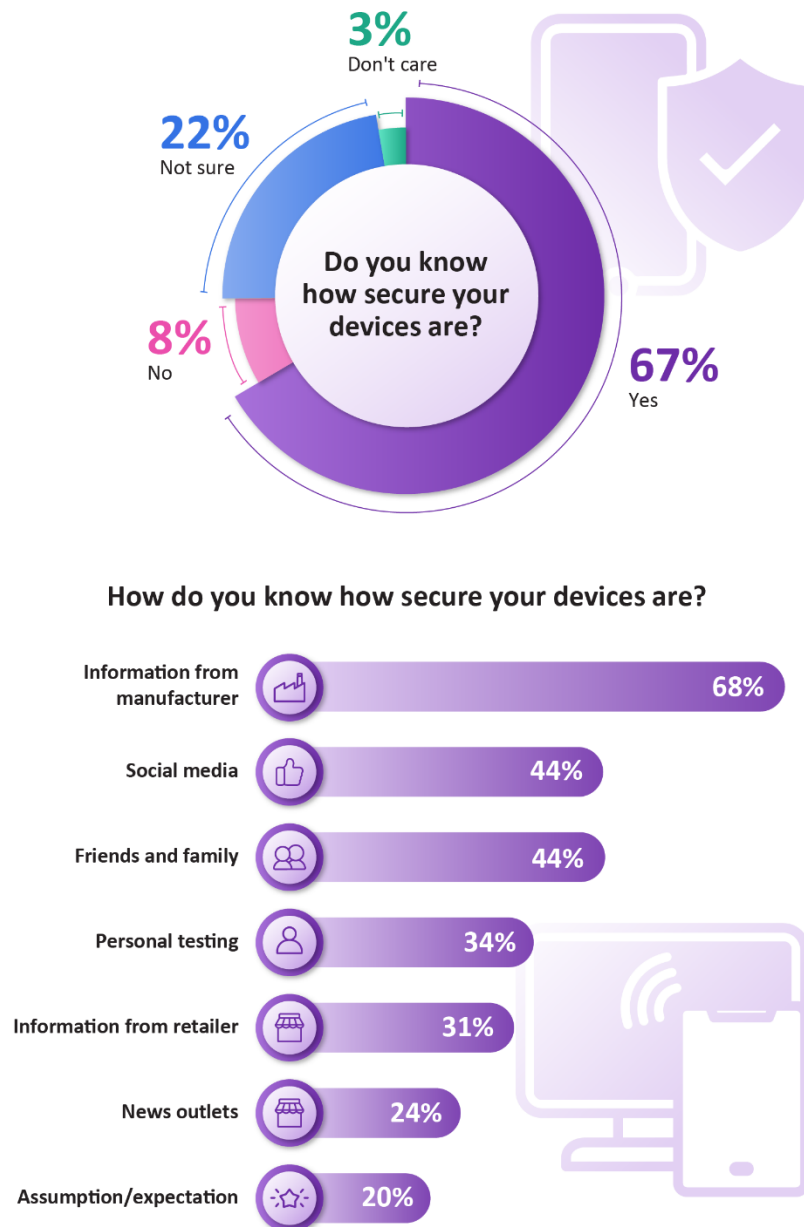
Notes: n=409, all regions.

© 2025 Omdia

Source: Omdia

Interestingly, 67% of respondents reported they understood how secure their devices were, with about that same percentage crediting manufacturer's information for that knowledge. While this echoed the earlier response regarding manufacturers' security responsibility, it was also clear that there are other sources trusted by consumers for device security information, including social media, friends, and family. This suggests that there is an opportunity to develop additional trusted sources of information on device security, so consumers can understand objectively what good security looks like.

Figure 22: Nearly two-thirds of respondents say they understand their devices' security



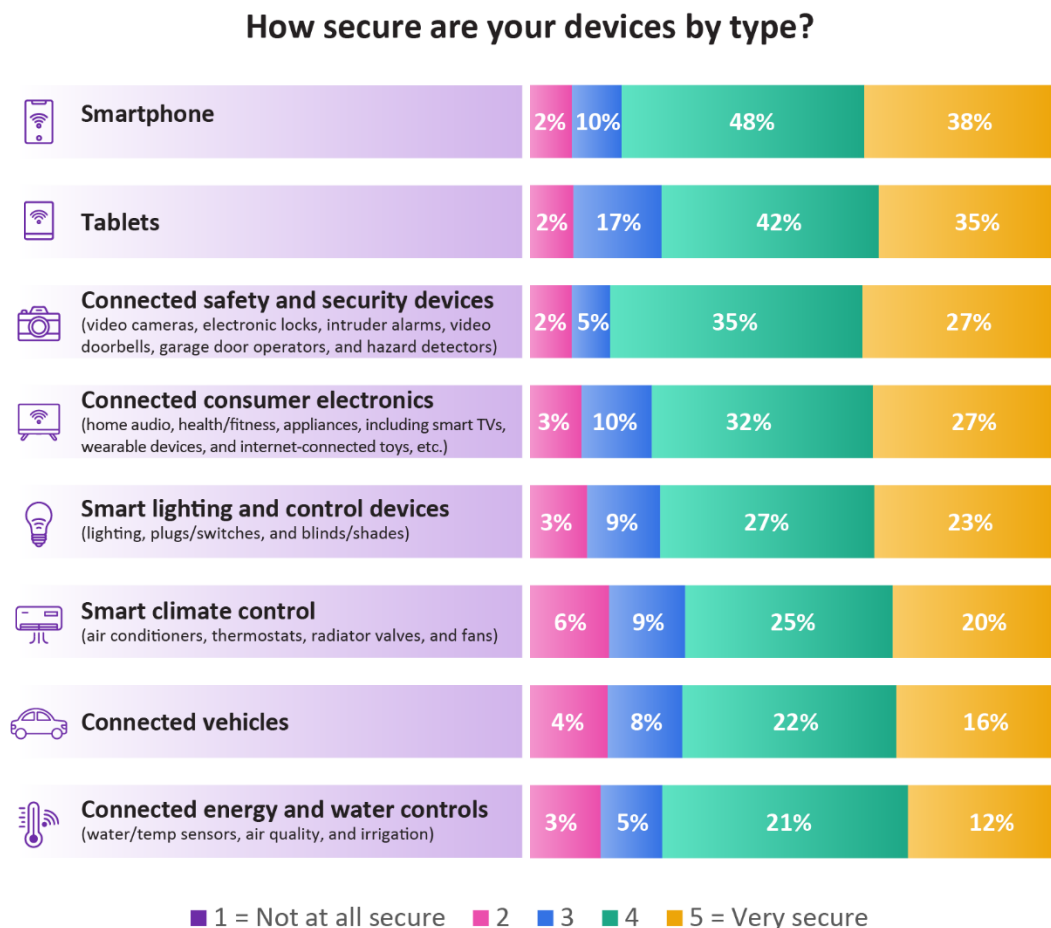
Notes: n=409, all regions.

© 2025 Omdia

Source: Omdia

Respondents' perceptions of how secure their devices are also varied by device type. While no device types were considered to be not at all secure, energy and water controls were rated as least secure.

Figure 23: Perceptions of security vary by device type



Notes: n=409, all regions.

© 2025 Omdia

Source: Omdia

When security concerns were asked about, data protection was the top-rated concern: more than 70% of respondents rated it a major concern or a concern. Data protection included personal data not being protected and related issues such as not having secure backups to protect the data and

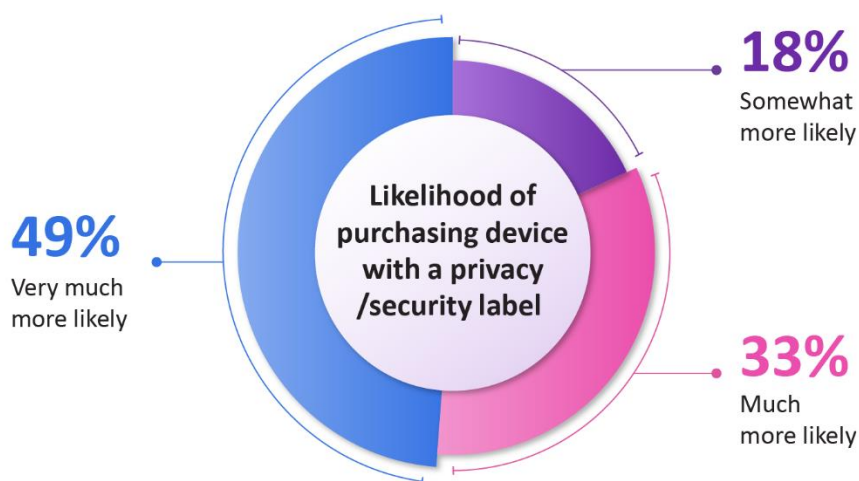
the inability to delete personal data. This reinforces that while ensuring data privacy is technically different from ensuring product security, these two areas are tightly linked in the minds of consumers. Other major concerns were default passwords (many IoT devices do not require users to change passwords) and malware protection, which does not exist on many basic IoT devices.

Although there was a lot of similarity in concerns across regions, there were some unique additional concerns that varied by country. For example, consumers in Germany were also concerned about the lack of physical access to devices, China users wanted better alerts for attacks and less vulnerability to outages, and US users wanted better lost device and anti-phishing protection. With variance across countries, it is clear it will be an ever-evolving process to create cross-cutting requirements that address everyone's needs.

Most respondents (64%) reported that they were either aware or very aware of standards and regulations requiring manufacturers and service providers to address security concerns. Additionally, a large majority (77%) said a device label that explains the privacy and security practices of the manufacturer would be important or very important.

Consumers also seemed willing to vote with their wallets: nearly all respondents were either very likely or somewhat likely to purchase a device with privacy and security labeling.

Figure 24: Likelihood of purchasing device with a privacy/security label



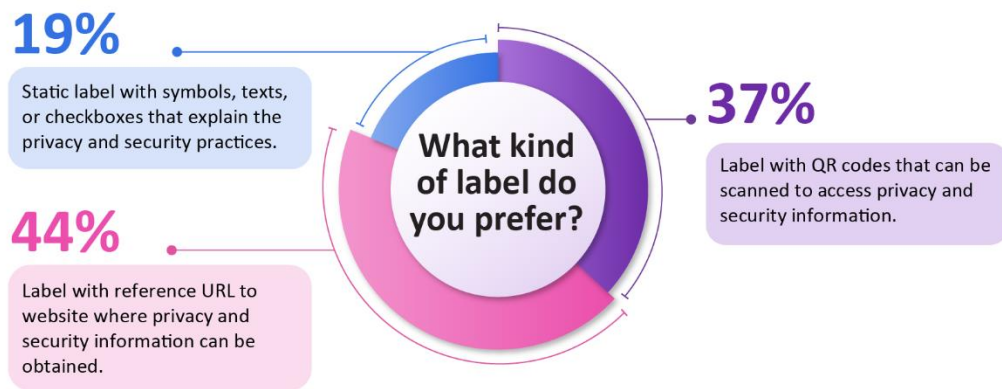
Notes: n=409, all regions.

© 2025 Omdia

Source: Omdia

In alignment with having more connected and digitally savvy consumers, the majority of respondents were also in favor of having dynamic and up-to-date information on a product’s privacy and security always available. Most (81%) preferred a label with either a reference URL linked to a manufacturer’s website or a QR code allowing them to get the latest data on any product.

Figure 25: Label preferences



Notes: n=409, all regions.

© 2025 Omdia

Source: Omdia

Conclusion: Time for reliably secure IoT products

Interviews with more than 400 consumers in 14 countries across regions indicated that most connected-device users not only recognize security concerns with their devices but also expect the manufacturer to provide solutions to them soon and make that clear through online verification available via a URL or QR code. Based on this survey, the manufacturers that do this will be rewarded with greater consumer interest and purchasing intent.

Still, apart from addressing consumers' top concerns, the question remains for manufacturers: how do they navigate the many country-specific standards, regulations, and schemes documented in this report? The recommendation based on the research of the initiatives across three regions and 16 countries is to look for ways to defragment and harmonize across the varied cybersecurity standards. It is recommended to use areas of more common ground as a basis, such as ETSI EN 303 645, because most of the countries researched are planning to adopt the guidelines.

Additionally, key national initiatives should be mapped to allow for nuances of compliance beyond ETSI. These include NIST, ISO/IEC, and major mandatory regulations that are expected from China and other countries that have not aligned to ETSI.

Consumers clearly want and value strong privacy and security. At the same time, governments and regulators are keen to protect their citizens from attack and protect citizens' digital sovereignty. The IoT industry must work with standards groups and governments around the world to make sure IoT has the robust security we all need and deserve. The CSA is stepping up to this responsibility by developing a global IoT cybersecurity certification program that is leveraging a superset of requirements to help harmonize across the varying baseline standards and emerging regulations.

Appendix

Methodology

This report, compiled by Omdia, is based on secondary research; interviews with regulators, suppliers, and standards bodies; and a random survey of more than 400 consumers across 15 major countries to determine device usage and security preferences. Survey qualification was based on usage of at least one other connected device beyond a smartphone or tablet.

Further reading

["Consumer IoT security," ETSI \(retrieved 2025\)](#)

["ETSI EN 303 645 V2.1.1 \(2020-06\)," ETSI \(retrieved 2025\)](#)

["ETSI TS 103 701 V1.1.1 \(2021-08\)," ETSI \(retrieved 2025\)](#)

["ETSI TS 103 621 V1.1.1 \(2022-03\)," ETSI \(retrieved 2025\)](#)

["ETSI EN 303 645 V3.1.3 \(2024-09\)," ETSI \(retrieved 2025\)](#)

["ISO/IEC DIS 27402 Cybersecurity — IoT security and privacy — Device baseline requirements," ISO/IEC \(retrieved 2025\)](#)

["ISO/IEC 27403:2024 Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics," ISO/IEC \(retrieved 2025\)](#)

["ISO/IEC DIS 27404, Cybersecurity – IoT security and privacy – Cybersecurity labelling framework for consumer IoT," ISO/IEC \(retrieved 2025\)](#)

["Cybersecurity Labeling for Consumers: Internet of Things \(IoT\) Devices and Software," NIST \(retrieved 2025\)](#)

["NISTIR 8425: Profile of the IoT Core Baseline for Consumer IoT Products," NIST \(retrieved 2025\)](#)

["Foundational Cybersecurity Activities for IoT Device Manufacturers," NIST \(retrieved 2025\)](#)

["Recommended Cybersecurity Requirements for Consumer-Grade Router Products," NIST \(retrieved 2025\)](#)

Author

Hollie Hennessy

Principal Analyst, OT & IoT Cybersecurity

hollie.hennessy@omdia.com

Get in touch

www.omnia.com
askananalyst@omnia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together “Informa TechTarget”) or its third party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.